



The Technology Capacity Project Guide

Strengthening your
technology systems
to better serve
your community



Contents

About This Guide.....	1
→ Who is This Guide For?	1
→ Using the Guide	1
→ How This Guide Will Help You to Do Your Job.....	2
→ What You Will Be Able to Do With This Guide.....	2
→ Before You Begin — A Note About Windows	2
Standard 1: Establish Strategy, Policies, and Documentation.....	3
Section 1: Technology Strategy and Planning	4
→ Why Do I Need a Technology Strategy?	4
→ What is a Technology Strategy?	4
→ How Do I Develop a Technology Strategy?.....	5
→ Developing Your Technology Strategy	6
Section 2: Inventory and Assess Your Technology Resources.....	10
→ Why Document Your Technology Resources?	10
→ What to Document	11
→ How to Document Your Technology	11
→ Inventory and Assessment Resources	11
Section 3: What to Consider When Investing in Hardware or Software	12
→ Investing in Hardware or Software	12
→ Hardware Basics.....	13
→ Software Basics	23
→ Installing and Maintaining Software.....	28
→ Network Basics	30
→ Server Basics.....	36
→ Website Basics	45
Section 4: Budgeting for Technology	51
→ What to Include in Your Budget.....	51
→ Understanding Total Cost of Ownership (TCO).....	52
→ Understanding Return on Investment (ROI)	52
→ Additional Resources	53

Standard 2: Secure Network and Data	54
Section 1: Documenting Support and Maintenance Systems	55
→ Who Takes Care of Technology in Your Organization?	55
→ Technology Job Descriptions	56
→ How Do You Communicate About Technology?	56
Section 2: Collecting and Reporting on Data	58
→ Storing and Using Data	58
→ Common Tools to Collect and Analyze Data	59
→ Next Steps to Be More Data-driven	59
→ Advanced Data Usage	60
Section 3: Security and Privacy Basics	61
→ Why Data Privacy and Security Matter	61
→ Understanding Security Threats	62
→ Documenting Data Privacy Policies and Procedures	63
→ Best Practices to Help Keep Data Secure	65
Standard 3: Implement Network Support and Maintenance	76
Section 1: Securing Your Assets	77
→ Secure Technology Assets Checklist	77
Section 2: Maintaining and Supporting Your Systems	78
→ User Support	78
→ Internal Support	79
→ External Support	80
→ Additional Resources	83
Standard 4: Update and Sustain Network Assets and Infrastructure	84
Section 1: Update Network	85
Section 2: Disaster Planning	86
→ Documentation	86
→ Unified Communications	86
→ Backup	87
→ Human-Made Disasters and Accidents	88
→ Disaster Planning Checklist	89
→ Conclusion: Becoming Flexible by Default	90
Section 3: Revise Your Technology Budget	91

Standard 5: Incorporate Cloud & Social Media Asset	92
Section 1: Cloud Computing for Nonprofits	93
→ What is Cloud Computing?.....	93
→ Basic Types of Cloud Computing	93
→ Advantages and Drawbacks of Cloud Computing	94
→ Types of Cloud Applications for Nonprofits.....	95
→ A Few Tips for Going Into the Cloud	97
→ Learn More	97
Section 2: Social Media Practices for DV Organizations	98
→ Using Social Media Safely.....	98
→ Developing a Social Media Strategy.....	98
→ Developing a Social Media Policy	99
→ Additional Resources	100
Conclusion	101
Contributors	102
Appendix	104
TechSoup IT Baseline Standards Goals, Objectives and Process for DV Agencies	105
Baseline Goals	105
Baseline Objectives	105
TechSoup IT Baseline Standards	106
Secure Network and Data.....	107
Implement Network Support and Maintenance	108
Update and Sustain Network Assets and Infrastructure	108
Incorporate Cloud and Social Media Asset	109
Job Profile: Information Technology (IT) Manager	110
Job Profile: Accidental Techie	112
Job Profile: Information Systems Director	114
BSAV Product Offerings	115
→ BSAV Recommended Hardware.....	115
→ BSAV Software Favorites.....	115
How to Request Your Donation With TechSoup	
Technology Capacity Building: E-Learning Series	
How to Use TechSoup Forums	
The Technology Capacity Project Toolkit	

About This Guide

The Technology Capacity Project Guide contains information, resources, and recommendations geared toward the technical concerns most pertinent to DV organizations small and large. This Guide is a collection of tools and information based on the ideas and feedback from California DV staff and TechSoup's technology experts throughout the world. We compiled information and tools that complement one another and hopefully make implementing the Baseline Standards easier.

The Guide is divided into five sections that align to the Baseline Standards as well as introductory content so you are aware of what is included in this Guide and how to best use these tools. It also includes a "Getting to Know the Gear" section, which provides basic introductions to hardware, software, servers and networking, Internet service, and your website.

→ Who is This Guide For?

This Guide is written for DV organizations that have little or no technical support. At the same time, understand there are DV organizations that have support resources (e.g., outside contractor, volunteer, etc.). If you fit in this category, it's very important that you meet with these people and discuss these recommendations and how you plan to update your system. They might have different plans in mind, so, in short, you need to work with them.

→ Using the Guide

You can use this Guide in a number of different ways. If you are new to overseeing and managing your computing environment, you should begin here and work your way through each section in turn. If you are more experienced but want certain information on a particular topic, you can go directly to the relevant section and review that material.

→ **How This Guide Will Help You to Do Your Job**

We recognize that DV organization staff members have a challenging job when it comes to keeping their computer system up and running. Typical issues include:

- Not having enough time
- Not having enough resources (financial)
- Limited resources to help with Information Technology (IT) problems and decisions

In response, TechSoup and the DV community have developed a recommended baseline for what you most need to pay attention to when it comes to managing and building your IT systems. This Guide will focus on those standards and provide you with directions and ideas for managing your systems.

→ **What You Will Be Able to Do With This Guide**

As mentioned before, this Guide targets the baseline standards with an end goal of helping your organization build a strong foundation and a healthy and secure IT system. Our assumption is that by adopting or implementing these standards, your organization will be better able to:

- Plan for and implement transformative technologies
- Integrate IT with programmatic functions
- Lower basic IT support costs
- Improve reliability of IT systems

→ **Before You Begin — A Note About Windows**

As you will notice, many of the recommendations in this Guide are for Windows-based computers. While we don't endorse Windows as the platform of choice, the overwhelming majority of DV organizations that we spoke with have Windows-based computers. Thus, it seems to be the most useful platform for the widest audience.

We are also focusing our recommendations on Windows 7. While there are organizations that still use Windows XP and Vista, we recommend that you upgrade these computers to Windows 7.

Standard 1: Establish Strategy, Policies, and Documentation



Section 1: Technology Strategy and Planning

→ Why Do I Need a Technology Strategy?

You have a mission. You work hard to make a difference for something you believe in. You also work hard to get others to believe in your work and support you.

The reason you should care about technology strategy and planning is that technology can work with you in supporting your mission — and getting others to support you. Is it going to magically fix all your problems overnight? No. But there's a lot it can do — from helping your organization work more effectively to helping you engage donors and funders.

A clear technology strategy can:

- Focus and guide technology conversations by making sure technology decisions are aligned with and support your organization's mission
- Inform and support good technology decision-making
- Help you prioritize your technology needs
- Help you clearly articulate your technology needs to potential funders and donors
- Be proactive, rather than reactive, in making technology decisions. For example, rather than making last-minute technology decisions when something breaks (your server, an old computer, your organization's website), you can plan ahead to maintain and upgrade your technology.

→ What is a Technology Strategy?

A *technology strategy* is a short document outlining organizational strategic goals and how technology can support those goals over a two- to three-year timeframe. Ideally, your technology strategy should also have clear objectives for meeting those goals, including budget, funding sources, staffing assignments, and a timeline.

Your technology strategy and planning should be connected to your larger mission as an organization. Remember, technology is not a goal in and of itself. Technology is important because of *what it allows people to do*: tell stories, exchange knowledge, and serve your mission and your community. Your technology strategy will be more useful and meaningful, as well as more convincing to potential funders, if it is clearly grounded in your mission.

Technology Strategy Resources

- [Forget the Tech, Let's Talk Mission](#) is a great introduction from NTEN on making technology relevant to the organization's mission
- Strategic Technology Plan Template included in the Toolkit

→ How Do I Develop a Technology Strategy?

The first steps in making a good technology strategy have nothing to do with technology. In fact, being "techy" can sometimes be a hindrance, as it can lead you to focus too much on the technology itself, rather than what technology can allow your organization to do. So, where does one get started in developing a solid technology strategy?

There are five main steps:

Step 1	Understand where you are. This includes reviewing your organization's strategic plan and mission statement, performing basic tasks like completing a technology inventory and assessment, and having conversations within your organization about how your organization's work gets done.
Step 2	Understand where you want to be. What is and is not working well in your organization? What kind of technology improvements might help?
Step 3	Identify technology solutions and prioritize them.
Step 4	Lay out a plan for funding and implementing technology changes.
Step 5	Write up your technology strategy.

Developing and implementing a technology strategy isn't quick or easy. Here are a few tips for making the process go more smoothly:

- **Know who you need to talk to.** Who should provide input into the technology planning process? Think about stakeholders both inside and outside your organization.
- **Designate a point person.** One person should be in charge of overseeing the process. This is not necessarily a technical role but a management role. This person may also communicate with and oversee consultants who implement technology projects.
- **Break projects into tasks.** Make sure the individual steps are clear so you can monitor progress.
- **Assign responsibilities.** Make clear which staff member will carry out which task.
- **Establish a timeline.** Set milestones and target dates for different phases of your plan.
- **Evaluate your success.** Evaluation should be built into any planning process, and technology planning is no exception. Decide beforehand what indicators of success you will look for. Build evaluation checkpoints into your timeline.

→ Developing Your Technology Strategy

Step 1: Understand where you are.

The first step to developing a technology strategy and making a technology decision is understanding where you are right now. Gather up the following documents:

- Your organization's strategic plan and mission statement.
- *TechSoup IT Baseline Standards*. Review the standards and determine where your organization is and what you've already accomplished. The standards document can be found in the Appendix.
- The technology inventory worksheets included in the Toolkit.

Mission First

Review your organization's mission statement and strategic plan. Ultimately, that's what the tasks and information in this Guide are all about: supporting you and the work you do that supports your mission. Technology is just another tool to help you do your organization's good work.

Inventory and Assess Your Technology

A technology inventory and assessment helps you develop a clear picture of the current technology situation in your organization.

Inventory and Assessment Resources

- Review the *TechSoup IT Baseline Standards* (found in the Appendix). Have you already completed some of the steps included in the Baseline Standards? Congratulations!
- The Toolkit includes detailed inventory worksheets and can be found in the Appendix.
- The "Getting to Know the Gear" section of this Guide provides an introduction to some of the major components of your organization's technology setup, including hardware, software, servers and networking, Internet service, and website basics. Knowing these basics will make inventorying your technology easier.

Start Having Conversations

A basic inventory of the computers, software, networks, and other technology your organization is using is just part of the puzzle. The other piece is *understanding how well your technology is currently working*. This involves assessing your technology and having conversations with people about the work they do and the technology they use to do it.

- Who do you need to talk to? Staff, certainly, but possibly also volunteers, clients, funders, donors, and others who are connected to your work.
- What do you talk about? One of the main things to talk about is process: what people do, how they do it, and how they think it could be done better. Don't get too hung up on specific technology tools yet – that will come later. The key thing to understand at this stage is what people need to do and what they would like to do better.

Assess As You Go

As you're inventorying your technology and having conversations with people, make note of what is working well and what is not working well, technology-wise. What are the strengths and weaknesses of your current technology? What processes could work better? Is there anything your organization would like to be doing but cannot do currently due to technology limitations?

Step 2: Understand where you want to be.

Now that you know what tools you're using in your organization and what is and is not working well, you can start thinking about where you want to be.

- Review the *TechSoup IT Baseline Standards* (in the Appendix). They can help you think about goals and next steps that might be appropriate for your organization.
- When thinking about where you want to be, remember that all your planning should be deeply rooted in what will best support your mission. Technology may or may not be the solution to your organization's needs.

A key thing when defining where you want to be is to describe *what you want to do with technology*, not what you think you need to buy.

- Start by thinking more abstractly about your organization's goals *before* you begin to discuss how technology might help you solve your problems and help your organization better fulfill its mission.
- Consider current and upcoming activities: day-to-day operations, new policies to institute, procedures you need to follow to find funding or comply with regulations, new staff to train, etc. Then consider all the potential tools, including technology tools, that you might use to solve these problems.

After you've clearly identified what you would like to do as an organization, begin thinking about where technology can help you accomplish those goals.

The following are two examples of the kind of language you might use to describe your technology needs. Again, the focus is not on a specific tool (e.g., an Access or FileMaker database, using Joomla to build a website). The focus is on what you need technology to *do*:

We are a community-based organization that provides comprehensive services to people who have suffered domestic violence. We require a secure central database to manage and track client information. Having one database will save time that is now wasted in multiple entries of the same data and will create one accurate source for all client information.

We are a domestic violence support organization located in an area with an increasingly high percentage of Spanish-speaking residents. To address this population's needs, we plan to update our website to provide information and resources in Spanish as well as English.

Step 3: Identify technology solutions and prioritize them.

Once you have assessed your resources and defined your needs, the next step is to make a concrete plan for how to meet those needs.

Identify Potential Technology Solutions

This is where you start thinking about specific technology solutions. For example:

- How secure is your technology setup? Are there any gaps that should be addressed?
- Are there better data storage and collaboration solutions available?
- Will upgrading to more recent hardware or software help?
- Is there a tool out there that will fill in a gap in your toolset?
- Would it help if your staff were trained (or retrained) in how to use your technology?
- What technologies are available to meet those needs?

Before you decide on a solution, you need a basic understanding of technology options. This Guide provides basic information on a variety of technology topics. You will also want to involve someone at your organization who has technology skills: a dedicated IT staff member, a consultant, a volunteer, or a tech-savvy staff member.

Prioritizing Technology Solutions

There are dozens of options with different price tags for each technology decision, so negotiating your priorities can get very tricky. The important thing is to go back to your original vision of how technology can help you accomplish your mission. What are the highest priority needs that technology will help you meet?

Resources

- [TechSoup](#), [Idealware](#), and [NTEN](#) are great sources for articles, blogs, and discussion forums on technology topics. All are geared towards a nonprofit audience.
- The TechSoup articles [Learning About Technology Online](#) and [Learning About Technology Offline](#) offer many other suggested resources for learning about technology.
- Learn the basics in the "Getting to Know the Gear" section of this Guide.

Step 4: Lay out a plan for funding and implementing technology change.

Your plan should include funding and budgeting, a timeline, and staffing resources.

- **Budget:** No technology plan is complete without a budget. Creating a budget is the only way to tell whether or not your plan is practical. Funding sources should also be identified. See *Section 3: Budgeting for Technology* and the Toolkit in the Appendix for additional information.
- **Timeline:** A timeline includes the phases of work and the deadlines for implementation of your plans.
- **Staff Assignments:** Outline who is responsible for the various steps in implementing your plans.

Step 5: Start writing!

If you've used the basic tools included in the Guide, you should now have everything you need to write up your technology strategy. The Strategic Technology Plan Template included in this Guide is a good place to start.

Finally, keep in mind that your technology strategy is not static. It should be a living, breathing document. As new needs and priorities come up, you can (and should) modify the strategy accordingly.

Section 2: Inventory and Assess Your Technology Resources

Knowing what technology assets and systems you currently have is an essential foundation for all other activities. In this section, we will discuss the benefits of documenting your technology resources and policies, and we will provide tips and tools for conducting a technology inventory.

→ Why Document Your Technology Resources?

Good documentation has many benefits:

- **Saving time.** Having all of your IT information in a single, central location will save you countless hours of frustrated searching for software license numbers, activation keys, and tech support contact information.
- **Efficient upgrade and maintenance planning.** How many PCs in your organization are more than four years old? Which computers need an update because they have old software? Which machines don't have enough RAM to run Microsoft Office 2010? You can answer all of these questions with a good technology inventory.
- **Better budgeting.** If you always have an up-to-date inventory of your current hardware and software, it's much easier to predict your future requirements.
- **Get the most out of your software and hardware.** Knowing exactly what technology you have means you're better positioned to take advantage of all that those tools offer. For example, Microsoft offers substantial [Software Assurance](#) benefits, including free software upgrades and free online training courses. Knowing what software you have and where it is installed also helps ensure you comply with software licensing requirements.
- **Standardizing your technology.** After you have an up-to-date inventory of your hardware and software, you may notice that you are running different operating systems and productivity software or have very different hardware on your computers. An inventory helps you establish a baseline and helps ensure that new technology investments meet that baseline standard.
- **Identifying critical procedures or policies that might be missing.** For instance, what kind of password policy do you have? Do you have a regular backup routine in place? Do you have a disaster recovery plan?
- **Disaster recovery.** In the event of a disaster, good documentation can help you get your critical technologies back up and running.

→ What to Document

An *inventory* is a specific, detailed description of what you own and where it is located. Your technology inventory should include desktop hardware and software, servers and network information, and technical support and vendor contact information.

An *assessment* is qualitative: How well is your technology working? How well does it support your processes and your organization's mission?

Policies should also be documented. The highest priority documents we recommend are:

- Technology strategy
- Acceptable use, including email and Internet use
- Security
- Data Privacy

→ How to Document Your Technology

There are a several ways to inventory your technology.

- **For smaller organizations**, a manual inventory is probably the quickest and easiest option. This is just what it sounds like: you walk and around and look over your technology in person.
- **For larger organizations with complicated technology setups**, consider using automated tools for asset management. [Spiceworks](#) and [TechAtlas for Nonprofits](#) are free asset management and inventory tools. Tools like [KACE](#) and [GFI LanGuard](#) can be used to inventory and manage more complex technology setups. The time (and sometimes money) it takes to set up and learn these tools may be worth it, because it will save time and effort in the long run.

For manually inventorying your computers, both Windows computers and Macintoshes have easy-to-use tools that provide detailed information about the computer:

- **For Windows**, the System Information (SI) program provides access to a wealth of information about a computer. The system information application is at Programs > Accessories > System Tools > System Information.
- **For Macintosh**, the System Profiler program provides in-depth information about a computer. The System Profiler is located in the Utilities folder in the main Applications folder.

→ Inventory and Assessment Resources

- See inventory worksheets in the Toolkit

Section 3: What to Consider When Investing in Hardware or Software

A grasp of basic technology principles will aid your technology planning process immensely. This section of the Guide provides basic introductions to:

- Investing in Hardware or Software
- Hardware Basics
- Software Basics
- Installing and Maintaining Software
- Network Basics
- Server Basics
- Internet Service Basics
- Website Basics

→ Investing in Hardware or Software

Buying and setting up a computer is a big investment, and with so many different options available, it can be hard to figure out how to meet the technical needs of your organization and still stay within your budget.

This Guide will help you understand the questions to ask when shopping for a computer and investing in software. In the hardware section, you'll find a quick reference checklist with definitions of some basic technology terms (not too many!), as well as the minimum standards we recommend for computers. In the software section, you'll find definitions of key terms and tips for purchasing, installing, and maintaining new software.

To help you make the most of your Blue Shield donation request through TechSoup, this Guide also includes a list of recommended hardware and software products that are available through TechSoup donations (see Appendix).

A Reminder About Planning

A technology plan, technology budget, and technology strategy are all helpful tools to make sure you understand your current and future computing needs. If you've been following the Baseline Standards, you've probably already started working on (or even completed) these documents.

Tip 1: Know What You Have

To recap from Standard 1:

- An *inventory* is a specific, detailed description of what you own and where it is located. Your technology inventory will include all the software you use in your organization, as well as hardware, servers and network information, and technical support and vendor contact information.
- An *assessment* is qualitative. How well is your technology working? How well does it support your day-to-day processes and your organization's long-term mission?

Having a clear inventory and assessment of the software, hardware, and other technology you currently use is a crucial first step in planning for technology acquisitions. This allows you to avoid mistakes (such as duplicate purchases or incompatible software) and to plan future purchases more effectively.

Tip 2: Know What You Need to Do

The Baseline Standards also recommend developing a *technology strategy*, a short document outlining organizational strategic goals and how technology can support those goals over a two- to three-year timeframe. This document will likely contain some specific technology goals that should help guide your technology selections.

Regardless of whether you've written a formal technology strategy, you still need to be able to clearly articulate what you want your technology to do. What do you need to do as an organization and how will technology support those needs? A key thing when defining your technology needs is to consider *what you want to do with the technology*, not simply what specific tools you think you need to buy.

Remember that all your technology planning should be deeply rooted in an understanding of what will best support your mission. Technology is not a goal in and of itself. Technology is important because of *what it allows your organization to do*.

Tip 3: Prioritize (Put Out the Fires First)

Negotiating your technology priorities can be difficult. The important thing is to go back to your original vision of how technology can help you accomplish your mission. What are the highest priority needs that technology will help you meet? Are there any glaring problems you need to address first?

You can also review the Baseline Standards to help you think about goals and next steps that might be appropriate for your organization. Some of the highest priority items from the Baseline Standards include ensuring that your organization's technology is safe and secure by implementing regular scheduled backups, a firewall, antivirus and anti-spyware software, and encryption tools. Tracking and managing your organization's financial information should also be a high priority.

→ Hardware Basics

This section is designed to help you ask the right questions so that you can make informed decisions when acquiring computers for your organization.

If you just need a quick reference guide to computer hardware and the minimum standards TechSoup recommends, you can skip to "Get to Know Your Hardware."

1. Do You Need a New Computer?

It's possible some basic maintenance tasks or a simple hardware upgrade can boost performance and give your old computer new life. See [Upgrading Your Computer Components](#) for additional information.

2. How Will You Be Using the Computer?

If you do need a new computer, one of the most important things to consider is *how you will actually use it*.

- **What kind of work will your staff be doing?** Basic office tasks, like creating documents and spreadsheets, checking email, and using the Internet? Or heavy-duty work with video, audio, or images? Audio-visual work tends to be resource-intensive and will require a more robust computer.
- **Will your staff be traveling** or only using the computer in the office?
- **How does the computer fit in with your existing technology?**
 - What operating system(s) do you use? Operating systems use up most of your computer's resources. If you barely meet the minimum hardware standards for using your operating system, you may not have the computing resources to do a lot of other tasks at the same time (multitask).
 - What software do you use? Do you have software that only works with a certain type of computer or only runs on a particular operating system?
 - 32-bit or 64-bit? The key thing to know is that hardware and software come in 32-bit and 64-bit versions. If your computer has a 32-bit operating system or hardware, you cannot run 64-bit software on it.
- **What are your future plans?** Are you planning to upgrade your operating system or add a new kind of software? Are you planning to do different kinds of tasks in the next couple of years?

3. Mac or PC?

The choice between Mac and PC often comes down to personal preference. Both types of computers have their merits. Macs and PCs use the same kinds of internal processors, so they are equally powerful. The main difference between Macintoshes and other computers is the operating system they use: Macintosh computers run Mac OS X (the latest version is called Lion) and PCs run Windows (the latest version is [Windows 7](#)). The Software section includes more information on operating systems.

A few things to keep in mind:

- **Macintosh computers are usually more expensive off the shelf than a similar PC;** however, some argue that the long-term cost for a PC is actually higher, due to additional software and maintenance costs.
- **There is some software that will only run on Windows.** Make sure the software you depend on is compatible with your new computer's operating system.
- **The more similar your computers are the easier your technology will be to manage.** If you have different types of computers, running different operating systems and different software, troubleshooting and maintenance become much more complicated. Consider whether you already have a Mac- or PC-centric office and whether it's worth switching some or all computers.

4. New, Used, or Refurbished?

If you plan to use the computer for basic office tasks like word processing, email, and web browsing, you probably don't need a top-of-the-line or brand new computer. A used or refurbished computer may be just fine. Used and refurbished computers are usually much less expensive than new computers. They're also a greener option, since you're extending the life of an old computer rather than buying a brand-new one.

A refurbished computer may be a better option than a used or donated one. Refurbished computers are older machines that have been carefully inspected and updated by professionals. If you get your refurbished computer from an authorized professional refurbisher (and you always should), you will know it is in good working condition. Refurbished computers also often have a warranty of some kind. Read more about refurbished computers available to eligible organizations through TechSoup's [Refurbished Computer Initiative](#).

There are some additional things you need to think about when buying refurbished equipment:

- **Failure and return rates.** Check the refurbisher's failure and return rates.
- **Warranty.** You probably won't get a three-year warranty for a refurbished computer, but a three-month warranty is pretty standard. This should cover any out-of-the box problems.
- **Peripherals, software, and documentation.** Make sure you know what is included with your computer. Refurbished computers, for example, rarely come bundled with a monitor.

If you are buying a used (rather than refurbished) computer or accepting a donated one, make sure a knowledgeable person inspects the computer thoroughly first. This will help ensure the computer is functioning properly and that it will meet your needs. Remember that as alluring as a free or very cheap computer might seem, an old one in poor condition can actually be more trouble than it is worth. Learn more about how to avoid receiving time-wasting donated hardware in [Six Tips for Accepting \(and Refusing!\) Donated Equipment](#).

5. Laptop, Desktop, or Tablet?

When deciding whether a laptop, desktop, or tablet (hand-held) computer will best meet your needs, the key things to consider are:

- **Price.** Laptops are usually more expensive than an equally powerful desktop computer, even if you factor in the cost of a monitor for your desktop. Parts and repairs are usually more expensive for laptops and tablets as well.
- **Travel.** If you will only be using the computer in the office, a laptop probably isn't worth the added cost.
- **Upgrade, repair, and maintenance.** Especially if you're planning to do this yourself, keep in mind that fixing or upgrading a desktop computer is much easier than a laptop or tablet.

- **Size or "form factor."** Desktop computers can be the traditional bulky tower, compact models that are smaller than a loaf of bread, or an all-in-one model (where the computer and the monitor are all one piece). Laptops come in different sizes, too: from tiny netbooks with miniature keyboards and 10-inch screens to ultra-thin or ultra-portable models to giant models with 17+-inch screens that don't even need a separate monitor. A few things to consider:
 - If you will be traveling a lot, size and weight are important considerations for laptops.
 - Smaller models are often more costly than a comparably equipped standard-size model.
 - There is often a trade-off between small size and computing power. Inexpensive netbooks, for example, may not be powerful enough to serve as your main computer.
 - Tablets (as handy as they can be and as popular as they are) aren't suitable for heavy use for office productivity tasks, but they're great for web surfing, checking email, and reading documents on the go.
 - For more information, [Consumer Reports](#) has a really nice, clear discussion of the pros and cons of laptops, desktops, and tablet computers, in varying sizes.

Get to Know Your Hardware

There are a few key things you should understand when you're making a decision about which computer to buy. We'll define them and provide the minimum standards you should be looking for to support performing basic office tasks.

COMPONENT	DEFINITION	KEY CONSIDERATION	MINIMUM STANDARD
CPU (Central Processing Unit) <i>Also known as processor</i>	This is your computer's brain, and its function – as you might imagine – is to process information. Usually, a faster processor means a faster computer.	Performance, which is based mostly on: Number of cores (single, dual, quad, and so on). Processor speed or "clock speed," which is measured in Gigahertz (GHz).	Dual-core processor with mid-range clock speed (2.6 GHz)
RAM (Random Access Memory) <i>Also known as: memory</i>	RAM is used to temporarily store information while your computer is running. More memory allows your computer to run more quickly, up to a point.* Confusingly, <i>memory</i> is not the same thing as <i>storage</i> (see below for additional information). Storage is what allows you to keep files and software stored long term, while memory is what your computer uses short term to perform its basic functions. <i>*32-bit operating systems can't use more than 4 GB of RAM, so if you have a 32-bit OS, you don't need more than 4 GB of RAM.</i>	Amount of memory, which is measured in Megabytes (MB) and Gigabytes (GB). There are 1024 Megabytes in a Gigabyte.	1 GB
Storage <i>Also known as hard-disk storage</i>	The amount of information (files, data, software, photos, video, and so on) your computer can store.	Amount of storage, usually measured in GB.	See <i>Hard Drive</i> below

COMPONENT	DEFINITION	KEY CONSIDERATION	MINIMUM STANDARD
<p>Hard Drive <i>Also known as hard disk, hard-disk drive (HDD), or internal drive</i></p>	<p>The hard drive is where most of the information on your computer is stored.</p> <p>There are two main types of drives:</p> <p>Traditional drives are spinning disks attached to a platter. Because the drive has these rapidly moving parts, hard drives are susceptible to mechanical failure. For example, when your drive "crashes," it's because the spinning disk literally crashes into the platter underneath it.</p> <p>Solid-state drives do not have moving parts and, therefore, are less likely to have mechanical problems. They are also faster and quieter than traditional drives, but they are also significantly more expensive.</p> <p>Note: An external hard drive is basically the same thing as an internal drive. An external drive just has a case surrounding it and a cable to connect it to your computer.</p>	<p>Disk size: the amount of storage space on the disk.</p>	<p>160 GB storage capacity</p>
<p>Networking</p>	<p>How your computer connects to the Internet or networked devices.</p> <p>An Ethernet port lets you plug your computer into a router for "wired" access.</p> <p>A wireless adapter or wireless card enables your computer to connect to the Internet and other devices wirelessly.</p> <p>Bluetooth is a technology that allows your computer to wirelessly connect to other devices, but it doesn't allow your computer to connect directly to the Internet.</p>	<p>Wired and wireless connection capability.</p>	<p>Ethernet port and a wireless card or adapter</p>

COMPONENT	DEFINITION	KEY CONSIDERATION	MINIMUM STANDARD
<p>Ports <i>Also known as output ports or interface ports</i></p>	<p>Device ports: How your computer connects to other devices, like a keyboard, mouse, printer, digital camera, or external hard drive. Different devices use different cables to connect to different kinds of ports. The most common ports and cables are:</p> <p>USB (Universal Serial Bus) – the current standard is USB 2.0, which provides a faster connection than the older USB 1.1 standard.</p> <p>Firewire (also known as IEEE 1394, iLink) provides an even faster connection for high-speed data transfer.</p> <p>Audio and video ports: How your computer connects to speakers and external displays, like a monitor or television screen. There are different kinds of outputs, including:</p> <p>VGA (analog) output is included on almost all desktops.</p> <p>DVI (digital visual interface) carries only video, not audio.</p> <p>HDMI (high-definition multi-media interface) carries both audio and video. Mini HDMI ports are often used on portable devices.</p> <p>Like HDMI, DisplayPort and Mini DisplayPort carry both audio and video.</p>	<p>What devices you will connect to your computer.</p>	<p>Device ports: Several USB 2.0 ports Audio and video ports: VGA port</p>

COMPONENT	DEFINITION	KEY CONSIDERATION	MINIMUM STANDARD
<p>Graphics Card <i>Also known as graphics processing unit (GPU)</i></p>	<p>The graphics card or chip is what allows your computer to process and display visual information (text, images, video, and basically everything you see on your computer screen).</p> <p>There are two main types of graphics processors: Integrated or on-board graphics cards are built into your computer, and they share your computer system's main memory.</p> <p>A dedicated graphics card has its own, separate memory.</p>	<p>Amount of system memory (RAM) and tasks you are performing:</p> <p>If you have at least 2 GB of RAM, integrated graphics should be sufficient in most cases.</p> <p>If you work with a lot of digital video, you will probably need more RAM and/or a dedicated graphics card.</p>	<p>Integrated graphics: fine for most everyday office functions</p> <p>Dedicated graphics card needed <i>only</i> if you're planning to work with a lot of digital media</p>
<p>Optical Drives <i>Also known as removable media</i></p>	<p>Optical drives let you read and record (or write) to CDs, DVDs, and Blu-Rays. A "burner" or "recorder," usually labeled "RW," allows you to record or write information to discs.</p> <p>Most drives are labeled with the type of discs they are compatible with, as well as whether they can record or write to a disc or only play or read it.</p> <p>Devices labeled "ROM" can only play discs; they cannot write to them.</p> <p>Devices labeled "RW" allow you to write information to discs.</p> <p>For example, a DVD-ROM/CD-RW can play DVDs and can both play and record to CDs.</p>	<p>What media you are using (CD, DVD, etc.).</p> <p>What devices can, and need, to read that data.</p>	<p>Functioning DVD-ROM/CD-RW device</p>

COMPONENT	DEFINITION	KEY CONSIDERATION	MINIMUM STANDARD
Peripherals	<p>Electronic equipment connected by cable (or wireless integration) to your computer's CPU.</p> <p>Monitor or screen</p> <p>Keyboard</p> <p>Pointing devices (mice, trackballs, touchpads)</p> <p>Printers, scanners, and other optional devices</p>	<p>For monitors, the key considerations are:</p> <p>Screen size.</p> <p>Display resolution is based on the number of pixels (the little dots that make up the image you see on screen) that can be displayed; more pixels means a sharper display.</p>	<p>15" desktop monitor (measured diagonally), 1024 x 768 screen resolution.</p> <p>Laptop screen size will depend on organizational needs; 1024 x 768 screen resolution.</p> <p>Fully functioning keyboards and pointing devices.</p>
Battery and Power Consumption	<p>When not plugged into an outlet, laptops use a rechargeable battery for power. Some laptops can have an extended battery added. This makes the laptop bigger and heavier but significantly extends battery life.</p> <p>Some laptops have batteries that cannot be removed, which makes them more costly to replace when the battery wears out.</p>	<p>Battery life: how long the battery retains power after charging.</p>	<p>No specific recommendation.</p>
Size or "Form Factor"	<p>Desktops, laptops, and tablets come in different sizes. Some desktop terms you may hear:</p> <p>Full-size: these computers are encased in a standard (sometimes bulky) "tower" case.</p> <p>Compact: smaller than full-size towers (sometimes called "mini-towers").</p> <p>All-in-one: the computer and the monitor are all one piece.</p> <p>While we use the term "laptop" in this guide, "notebook" means the same thing. A netbook is a very small, lightweight (and less powerful) laptop computer.</p>	<p>Unless you will be traveling a lot, size is not usually a major factor when choosing a computer.</p>	<p>No specific recommendation.</p>

7. Do Your Research

The following are good places to start your research:

- [Consumer Reports](#) provides an easy-to-understand, comprehensive computer buying guide and product reviews.
- [CNET](#) and [PC Magazine](#) have more detailed technical buying guides as well as computer reviews for laptops and desktops. Just go to their site and search for "computer buying guide," "laptop buying guide," or "desktop buying guide."
- Learn about 32-bit vs. 64-bit computers with TechSoup's article: [Do I Need the 32-bit or the 64-bit Version?](#)

When doing your research, keep your organization's needs, budget, and the minimum requirements in mind and ask yourself:

- Will this product meet our needs?
- What do you know about the company that makes the computer? Do they have a good reputation? What about the particular computer you're looking at?
- What kind of warranty do you get and how long does it last?
- How good is the company's technical support and how long can you use it?
- What other hardware comes bundled with the computer? A monitor, keyboard, mouse, cables?
- What software comes with the computer?

→ Software Basics

From basic office tasks to fundraising to tracking client services, nonprofits need software to get their work done. This section of the Guide will provide a quick introduction to some basic software terminology and provide tips for selecting, installing, and maintaining software at your organization.

First, a few quick definitions.

- **Traditional software** is software that is installed directly onto your computer or server, such as your computer's operating system or Microsoft Office.
- **Cloud-based or online software** is software that is hosted somewhere else, meaning it is not installed on your organization's computers. Usually, you access it over the Internet using a web browser. Related terms that you may hear are *web apps*, *cloud computing*, or *software as a service (SaaS)*. For much more information on cloud computing, see the Cloud Computing for Nonprofits section of this Guide.
- **Desktop software** is the term for software you install on your computer to perform everyday tasks like creating documents, storing and analyzing data, keeping your computer secure, and communicating with others. Desktop software includes things like the computer operating system, office productivity tools (word processing, email, database, presentation creation), graphic design, and antivirus and security software.

Many kinds of "desktop" software are also available in online versions or mobile versions.

- The **Operating System (OS)** is the basic software that allows your computer and your mobile devices to run. Most computers and other devices come with the operating system already installed, so you usually don't need to purchase the OS separately. However, your organization might get a donated or used computer that does not have the operating system installed, or you may need to change or upgrade your existing operating system.

Macintosh computers usually run Mac OS X (the latest version is called Lion), and PCs usually run Windows (the latest version is Windows 7). Linux is an open-source operating system, most often run on PCs. Regardless of which operating system you choose, you need to make sure your hardware and your other software are compatible with the new operating system.

Like computers, smart mobile phones also have different operating systems, including Apple's iOS, Google's Android, BlackBerry's operating system, and Microsoft's Windows Mobile.

A Note on Terminology

The terms software, app, and application are often used interchangeably. This can be confusing. "App" is short for application, and it can sometimes refer to something that is more limited or simpler than a full-fledged "application," sort of a mini or junior application.

More often, the word "app" is used along with "mobile" or "web" to describe how the software is accessed and used. A *mobile app*, then, is just a piece of software that was created to be used on a mobile device. A *web app* is software that you access and use online, either via a computer or a mobile device.

For purposes of the software guide, we'll use software as the umbrella term and use "apps" to refer specifically to the mobile and web app categories of software.

Planning For and Choosing Software

Tip 1: Standardize as Much as Possible

Standardization is a strategy that helps minimize technology costs by keeping hardware and software as consistent as possible and reducing the number of tools you have that do the same basic tasks. For example, if you've standardized your software, every computer in your organization would have the same operating system and the same office productivity tools.

Having software standards in place can help your organization:

- Streamline technology infrastructure and simplify decision-making.
- Reduce purchasing and maintenance costs.
- Reduce the burden on technical support staff. Each new piece of technology you bring on board has a learning curve. The troubleshooting and support skills needed for each piece of software are different.
- Avoid compatibility problems. The more different kinds of software you have, the more often you'll encounter conflicts and errors that are hard to isolate and fix.
- Improve communication. When there's no standard, it's harder for your technical support to communicate with your staff. Neither side really knows what the other is talking about.

A *standard image* is one way to help standardize your technology. This is a pre-defined set of software that is installed on each computer. This means that everyone has the same basic software, and you have a handy checklist to refer to whenever you get a new employee or a new computer.

Keep in mind, certain roles may require different software. For example, finance staff will require finance and accounting software that would not be relevant for other employees. Think through the different kinds of roles in your organization. You can probably come up with a standard image for each type of staff, and you can refer to the standard image when setting up new computers.

See the *Standard Image Sample Worksheet* in the Toolkit for an example.

Tip 2: Get Familiar with Software Licensing

Software licensing is a complicated topic, but the first thing to understand is that you don't actually own the software you're using (even if you've paid for it). Buying software is kind of like buying a DVD: you own the physical copy of the DVD, but that doesn't give you rights to the original screenplay or finished movie. It's the same with software.

In fact, you are actually only renting or *licensing* the right to *use* the software, often in restricted ways: for example, on a certain number of computers, for a defined number of users, for certain purposes, or for a defined time period. That's why using software often involves licenses and various legal agreements and contracts.

There are a few licensing terms it's helpful to be familiar with:

Free/Open Source vs. Proprietary Software

- **Free/Open source:** In a software licensing context, "free" doesn't have anything to do with price. It means free in the sense of "free speech" and refers to the rights and restrictions imposed on using software. "Open source" is slightly different from "free," but in general, if a program has a free or an open source license, you don't have to pay anyone or ask their permission to install it. You can also copy and redistribute the software to your heart's content.
- **Proprietary software:** If the software is proprietary or closed-source, you'll usually find significant restrictions in the license that limit the ways you can use the software, copy it, alter it, and redistribute it.

The **End-User License Agreement (EULA)** spells out the restrictions on software use. The EULA is that long mass of text that appears when you're buying or registering software. Almost everyone clicks "I agree" or "I accept" without actually reading the agreements. However, the EULA explains everything from what you can do with the software to what the software company can do with your data and what additional software the company can install on your computer. This means it's a good idea to review these agreements, but it's especially important to do so for one-off or small software purchases from less well-known companies.

Volume licensing: Most major vendors offer some type of bulk purchasing and volume licensing option for software. The terms vary, but if you order enough software to qualify, volume licensing can be cheaper and more convenient for your organization. Nonprofits sometimes qualify for volume licensing with very small initial purchases. Also, volume licensing often provides you with a central place to manage all your licenses for a particular product or group of products.

A **Client Access License (CAL)** is a specific type of license that allows "clients" (the technical term for individual users or specific devices like computers) to connect to and use server software.

Tip 3: Do Your Research

Below are a few questions to ask when you're researching a software purchase:

- Will this software meet our needs? For larger and more complex software purchases, you will want to develop detailed requirements as well as research and compare several different vendors. See the Additional Resources section to learn more about this type of planning and selection process.
- What do you know about the company that makes the software? Do they have a good reputation? What about the particular software you're looking at? Read and compare reviews before making a decision.
- What are the technical requirements for using the software? Is the software compatible with your existing hardware and other software? For cloud-based technologies, do you have a reliable Internet connection and enough bandwidth to use the software?
- Does the software meet your organization's security requirements?
- How many people will need to use the software?
- What are the up-front and ongoing costs?
- What licensing options are available? Is there a volume discount?
- Does the company offer special nonprofit pricing?
- How are patches, bug fixes, and upgrades handled?
- Is there a free trial available? Using a trial version of the software before purchasing can help make sure the software is compatible with your existing hardware and software and that it meets your organization's needs.
- What is the return policy, if any?
- What kind of tech support do you get? How long can you use it?
- What kind of training is needed to use the software effectively? Does the vendor provide good documentation or additional training resources?

Additional Software Planning and Selection Resources

Finding Donated and Discounted Software

- [TechSoup](#) offers many donated software options to qualifying nonprofits.
- [A Quick Guide to Discounted and Donated Software](#) provides other suggestions if your organization is not eligible for a particular TechSoup donation.

General Software Planning

- [Navigating the Nonprofit Software Selection Process](#) and [An Insider's List of 10 Things You Should Ask Before Buying Software](#) provide good tips for what to think about when buying software.
- Idealware's article [Selecting Software on a Shoestring](#) offers a "quick and dirty" approach to software selection.
- For larger purchases, TechSoup's article [An Overview of the RFP Process for Nonprofits and Libraries](#) explains the difference between an RFP (request for proposal), an RFI (request for information), and an RFQ (request for quotation), and provides guidelines to help you decide between a formal and an informal RFP process.

Specific Software

- TechSoup's article [Should You Upgrade to Windows 7?](#)
- TechSoup's article [What Your Organization Should Know about Office 2010.](#)
- Microsoft offers free online training courses as part of their [Software Assurance](#) benefits.
- [Idealware](#) is an excellent place for nonprofits to learn about software. Their "A Few Good Tools" series, for example, provides comprehensive, nonprofit-focused reviews of particular categories of software, such as [eAdvocacy](#) and [Online Backup](#) tools. Unlike most of their other resources, their [Field Guide to Software for Nonprofits](#) isn't free, but it is a very nice easy-reference guide for many different types of software.
- Idealware's article [Comparing Online vs. Traditional Office Software](#) is a good introduction to cloud-based productivity tools.
- Learn more about open-source software options in [Creating an Open-Source Desktop](#)

Licensing Resources

- [Javacool Software's EULAlyzer](#) is a tool that helps review and analyze license agreements by automatically flagging suspicious words and phrases.
- TechSoup's article [Making Sense of Software Licensing](#) provides much more detail on the different types of licensing.

→ Installing and Maintaining Software

Now that you've chosen your software, you'll need to install it before you can start using it. This section will provide an introduction to software installation and some tips for maintaining and troubleshooting your software.

Installing Your Software

The first step in installing your software is actually getting your hands on the software itself. You can access traditional software in two different ways: getting a physical copy of the software on an installation disk or flash drive or by downloading the software from the vendor's website. Cloud-based software often (though not always) won't require any installation, because the software and related information is all stored and managed on the vendor's servers.

Read TechSoup's article [A Beginner's Guide to Electronic Software Downloads](#) to learn more about downloading software.

Once you've acquired the software, you need to install it onto specific computers. You have a few options: you can install software individually on each separate machine or you can manage software installations centrally. If you are a small organization with only a few computers or only a few users need to use the software, installing software individually is fine.

But if you're a larger organization, you might want to consider centralizing software installation and management with a systems management software suite or software installers.

- **Systems management software** bundles together several different tools that can make an administrator's life easier. For example, it lets you specify standard, scripted answers to all of the questions that normally come up during the installation and setup process. With most systems management software, you don't even have to touch the computers you want to install software onto. The systems management software will push out software to the computers on your network and start the process automatically from your server. Systems management software can also handle other administrative tasks such as patch management, asset management, and network monitoring. These tools can be expensive as well as complicated to set up and maintain, so they are most appropriate for larger organizations with good in-house technology support. Microsoft's System Center Configuration Manager, [KACE](#), and [Novell ZENworks](#) are examples of systems management software.
- **Software installers** (often used with Windows systems) can also help you with software rollouts, but they're not as powerful as a systems management suite. [InstallShield](#) is an example of a software installer.

Before you install new software, it's a good idea to run a backup on your computer (and if you've been following the Baseline Standards, your computers are already being backed up regularly). That way, if something goes terribly wrong during the installation, your data is protected and can be restored. This is especially important when you're installing a new operating system.

Keeping Track of Software

Whatever system you have in place for tracking software licenses, use it to record the number of licenses you've purchased, the number of copies you've installed, and the location of the installed copies.

Also be sure to keep track of your installation disks, passwords, and license keys. If you have received a software donation from TechSoup, it can also be helpful to keep a copy of the fulfillment email. This email will usually include your product registration key (if needed), links, and other helpful information.

Tools for tracking software include:

- The Software License Inventory in the Toolkit.
- Volume licensing programs usually provide an online account that is automatically updated when you acquire or activate a copy of that company's software.
- As discussed in Standard 1, [Spiceworks](#) and [TechAtlas for Nonprofits](#) are free asset management and inventory tools. Tools like [KACE](#) and [GFI LanGuard](#) can be used to inventory and manage more complex technology setups.

Keeping Your Software Up-to-Date

Software patches and updates often fix security problems that could allow attackers to compromise your organization's computers. Keeping your software up-to-date is one of the easiest and most important things you can do to help keep your computer healthy and secure.

Most major software packages have an automatic update feature that will notify you when an update is available. In most cases, all your users need to do is click 'OK' and follow the on-screen instructions when the notification appears. For centralized patch and update management, systems management software and software installers can be used, as discussed above.

Software Troubleshooting Resources

Nothing runs perfectly. So, at some point, you will almost certainly have questions about your software or run into a problem. Below are some places you can get your software questions answered.

- Learn some software troubleshooting basics in TechSoup's article [Eleven Tips for Troubleshooting Software](#)
- Many software vendors maintain their own discussion forums. If you're having a software problem, it's a good bet someone else may have had the same problem or know of a great solution. Vendor forums can be very helpful when looking for specific answers to software questions or to learn how to fix software problems.
- The [TechSoup Forums](#) are another great place to ask technology questions. There are over 20 forums on topics like [Virus Vaccination and Computer Security](#) and [Volunteers and Technology](#).

→ Network Basics

This section will provide an introduction to basic server and networking concepts. Even if you plan to hire an external contractor or IT support person to help build or manage these technologies for you, understanding these basic concepts will help you better define your needs, evaluate proposed solutions, and understand any issues or problems that may arise. It will also help you communicate more easily with your technology vendors and IT support.

An Introduction to Networks

Networking technology can be a little intimidating, but it's a huge part of our everyday lives and an important part of how most organizations get their work done. If you have a shared file system, Internet access, or a shared printer at your office, your office is networked. Email and other communications are transmitted over the Internet, which is the biggest network of all (actually it's a whole bunch of networks that are connected to each other).

What is a Network?

A network is any interconnected group of people or things capable of sharing meaningful information. In a technology context, "network" usually implies that computers are the things doing the sharing.

Why Network?

Networks are important because they facilitate resource sharing and provide faster, easier access to information and communications. For example, a network lets you store an important report on a shared drive where everyone who needs the information can always access the most recent version (rather than, say, copying the report to a portable thumbnail drive and handing the drive to someone else). Rather than buying one printer for every employee, an organization with a network can buy a single printer, connect it to the network, and set it up so that every user in the organization can print to it.

Networks also allow you to share computing power by using a server. More on servers in the Server Basics section, below.

Types of Networks

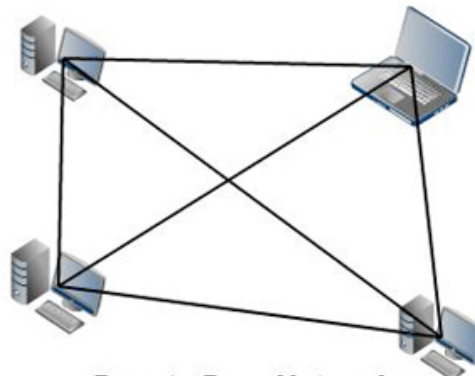
Different terms are used to describe how devices are connected together:

- A computer totally disconnected from other computers is a **standalone computer**.



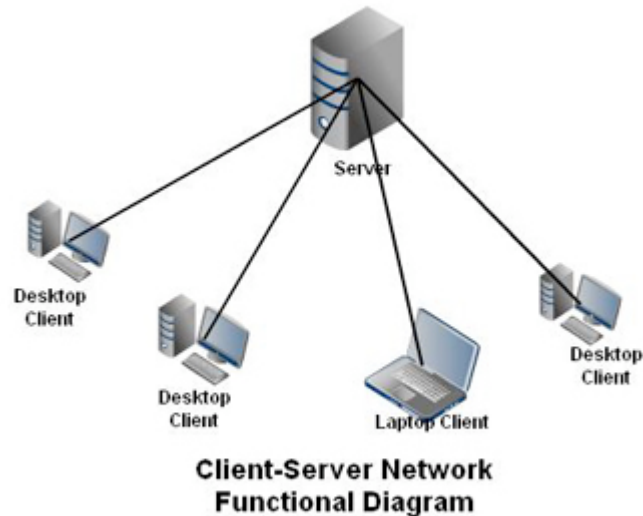
**Standalone
Computer**

- **Peer-to-peer:** A peer-to-peer network means multiple computers are connected to each other, rather than relying on a server to share information. In this type of network, every computer can communicate with all the other machines on the network, but, in general, each one stores its own files and runs its own software.

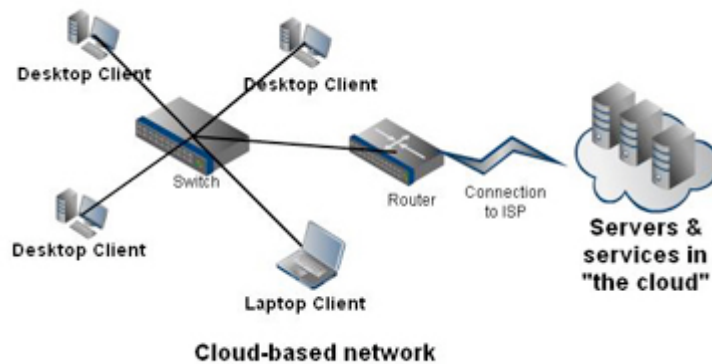


**Peer to Peer Network --
Functional Diagram**

- Client-Server:** With a client-server network, individual computers are called "clients," and the server performs critical functions on behalf of the clients on the network. These functions might include data storage or running large, shared, resource-intensive software such as databases and CRM software.



- Cloud-based:** In a cloud-based network, an organization's data, software, and other resources are hosted on servers outside the organization. The organization accesses and manages those resources via the Internet using a web browser. And because the servers and services are in the cloud, you don't need to be in the office or connected to your organization's network to access them.



There are also different terms that describe the network's scale or size:

- A local area network (LAN)** is a network designed to cover a single building or office, and its purpose is to connect and share computing resources within a single organization. LANs may be wired or wireless.

- A **wide area network (WAN)** connects a single office or branch's local area network to its parent organization's network.
- A **virtual private network (VPN)** is a way to allow staff to securely access information and resources on your network from outside your organization.

Key Networking Technologies

There are a few key networking terms and technologies you should be familiar with. In this section, we'll cover the protocols (or agreed-upon standards) for wired and wireless networking, basic computer and networking hardware, and how networked devices connect together.

1. Networking Protocols

The most relevant protocols for wired and wireless networking are:

- **Wired:** Ethernet (also called IEEE 802.3) is the group of technologies used in wired networking.
- **Wireless:** 802.11b/g/n (or WiFi) is the accepted standard for wireless networks.

2. Device Hardware

The hardware on your computer or other device that allows it to access a network includes:

- The **network card** (also known as a NIC or Network Interface Card) sends and receives messages and information. Each NIC has its own Media Access Control (**MAC) Address**. The MAC Address is a unique identifier for each device.
- The **Ethernet port** on your computer lets you plug your computer into a network for wired access.
- A **wireless adapter** or wireless card allows your computer to connect to the Internet and other devices and networks wirelessly.

3. Network Hardware

Network hardware is another important part of understanding your network. Network hardware includes appliances like hubs, switches, and routers. These all look kind of alike: a box with cables and a power cord sticking into it and a bunch of blinking lights on the front. But they do have different functions.

- A **hub** distributes messages and information among the computers and other devices on a single local area network. It's kind of like your network's mailman – it knows where messages should go and makes sure they get there.
- A **switch** (also known as a network switch or an Ethernet switch) is very similar to a hub, but switches have additional functionality such as network traffic control. A managed switch has even more features and functionality and offers more advanced security options for managing a growing network.

- **Routers** are kind of like the post office's regional distribution centers. They distribute messages and information beyond a particular network. There are too many locations in the world for a single switch to keep track of, so routers forward your messages and information to a router that is closer to the final destination, which then forwards it to another router and on to another until the message reaches its destination. Routers also offer the most security options and capabilities, including directing network traffic and controlling who can access the network and how they can access it.

4. Connecting It All Together

Finally, there are the connectors, the things that carry data and information across your network.

- Wired networks rely on cables to connect devices to each other. The most common types of cabling are Category (Cat) 3, 5, 5e, and 6. These are called "twisted pair" cables, because they're made up of two wires twisted together housed in a protective outer coating. A higher category number means the cable can carry more network traffic. Cat 3 cables are limited to carrying 10 Megabits per second, while Cat 6 can carry up to 1 gigabit per second. What kind of cabling you choose will depend on what kind of devices you are connecting and your existing network setup.
- Wireless networks transmit data and information electronically through the air. There are a variety of speeds and methods for devices to connect wirelessly, depending on which wireless standard you are using (802.11a, 802.11b, 802.11g, or 802.11n). The latest, fastest wireless standard as of early 2012 is 802.11n.

Setting Up Your Network

Now that you've got the basic terminology down, it's time to talk about planning for and securing your network and to discuss what a VPN can do for your organization.

Network Planning

The following are some questions that can help guide your network planning process:

- What networking infrastructure do you already have in place?
- How many computers and networked devices do you have?
- Does your office's design and layout impose any physical constraints on your planning process? For example, is there available space in your floors, walls, or ceilings where you can string your network cables?
- What networked software do your users rely on most heavily and how much bandwidth do these applications consume?
- Are you planning any changes to your technology infrastructure (such as additional employees or new software) that might have an impact on your networking needs?
- How much money do you have budgeted for the installation and maintenance of your networks?
- Do your users require the ability to access network resources when they are outside the network?

Securing Your Networks

The following are some steps you can take to help ensure your network is secure.

- **Understand your situation.** If you have already completed a technology inventory and assessment, as recommended in the Baseline Standards, you should be in a good position to answer all of these questions: Who uses your network? What types of hardware and software do they use? What kind of Internet connection does your organization have? Do you host your own website or your own email server? Do you allow staff to connect to your network with their own computers and other devices? What types of security policies, procedures, and equipment do you already have in place?
- **Identify risks and vulnerabilities.** Focus on protecting the high-impact, high-risk areas of your network. For more information, see [Identifying Vulnerabilities and Risks on Your Network](#).
- **Assess the risks.** The various vulnerabilities on your network represent potential costs — time, money, and assets — to your organization. These costs, along with the chance someone will exploit these vulnerabilities, help determine the level of risk involved. Risk assessment is a combination of both quantifying (the cost of the threat) and qualifying (the odds of the attack). Each organization will have to determine its own tolerance for risk.
- **Select and implement a security device** proportional to your networking needs. Depending on your networking needs, this may be a firewall, secure router, or other networking appliance that includes security features.
- **Have good basic security procedures in place.** The basic security procedures outlined in the Secure Network and Data section of this Guide are also crucial components of keeping your network secure: regular scheduled backups, a password policy, up-to-date antivirus and anti-spyware software, encryption technologies, and physical security.

Securing Your Wireless Network

Wireless networks are inherently easier to hack into than wired networks, so they require additional security precautions. When setting up your wireless network, take the following additional steps to help make your network more secure:

- Change the SSID (network name) from the default name.
- Change the default password to a stronger password.
- Enable WPA2 encryption. Encrypting your network traffic helps ensure that only authorized users will be able to understand the information being transmitted.
- Enable MAC filtering. The MAC address is the unique identifier for each computer, and you can limit access to your network to only a list of pre-approved devices based on their MAC address.

Setting up a VPN

Imagine that the Internet is a public highway. The information you transmit are the cars that move along this highway. Of course, your car isn't completely safe on a public highway, since someone could look inside your car, steal it, or crash into it. In much the same way, information traveling the Internet is neither safe nor secure.

A VPN is one way to handle transmitting information securely. A VPN is like a safe highway or a tunnel where cars — or your information — can safely travel. A VPN creates a secure, encrypted tunnel between a user's computer and the office network. It uses encryption to scramble the communication as it travels across the network and unscramble it when it arrives at its destination. This ensures that only authorized users can understand and use the data.

There are two kinds of VPNs: *remote access* and *site-to-site*. Remote access VPNs allow users outside the network to access an internal network by logging into their VPN as needed. Site-to-site VPNs create an uninterrupted connection between two different networks. Which you choose depends on how your organization works. If you have several offices that need to share information regularly, a site-to-site VPN may make sense. If you only have one office location or your offices mostly work independently, a remote access VPN may make sense.

VPN solutions can be hardware- or software-based, or a combination of both. Depending on the type of VPN you decide to implement, either remote-access or site-to-site, you will need different components to build your VPN.

For more information on VPNs and other remote access technologies, see TechSoup's articles "Demystifying Remote Access": [Part 1](#) and [Part 2](#).

Additional Networking Resources

- **General Networking:** TechSoup's Networking 101 series, starting with [Networking 101: Concepts and Definitions](#).
- **Wireless Networking:** PCWorld's [How to Lock Down Your Wireless Network](#) provides some good, basic tips. Their article [Lock Down Your Wi-Fi Network](#) goes into more detail.
- **Network Troubleshooting:** see Lasa's Network Troubleshooting three-part series: [Introduction](#), [Network Troubleshooting for Workstations](#), and [Network Troubleshooting for Servers](#).

→ Server Basics

Now that you understand a little more about networking, it's time to dive into servers. This section will provide an overview of servers: hardware, operating systems, and other server software, as well as what servers can do for your organization.

What is a Server?

The broadest definition is a server is a piece of software or hardware that provides resources to one or more computers or other devices on a network.

But the word "server" can be confusing, since it's used as a catch-all term for several different things: the physical server hardware itself, the server's operating system, and other software (called server applications) installed on the server.

We'll provide more detail on all these different components below.

Do I Need a Server?

A good rule of thumb is that peer-to-peer networks can be sufficient for small organizations with fewer than 5-7 computers, but they can quickly be overtaxed as the needs of an organization grow. If your organization has more than 5-7 computers, you might want to consider a server.

Other reasons to consider a server include:

- **Easier centralized administration:** A server can also help you manage the users on a network. All server operating systems offer "directory services," which allow you to create and manage user accounts, giving you greater control over who has access to your organization's information. For example, you can assign one user or a group of users access to a human resources folder but exclude others from opening it. Servers also help you centrally manage software installation and updates. For example, the free [Windows Server Update Services](#) tool allows you to distribute Microsoft software updates to computers in your network, selectively control which updates groups of computers get, and monitor the status of updates. Similar tools are available for antivirus and other security software.
- **Easier file and resource sharing:** A server facilitates sharing. One staff member can save files on a server and other staff can look at the file and work on it. A server is also designed to help share other resources such as databases and printers.
- **More data storage:** Servers are designed with storage in mind. Not only do most come equipped to store a lot of data, they also allow you to add additional storage capacity should you need it down the road.
- **Better backups:** Without a server, your staff is forced to save their work on their own computers, leaving files and folders scattered across a number of machines. As the number of computers in your environment increases, backing up these files can become more time-consuming and difficult to manage. Rather than backing up each machine individually, you can centrally manage backup using your server.
- **Improved performance:** Servers are designed to accommodate multiple users simultaneously. To boost performance, servers are equipped to handle more memory and processing power than a regular desktop computer. If sharing files or a database from another staff's computer in a peer-to-peer setup is slowing you down, it's time to consider a server.

Server Terminology

As mentioned earlier, people use the term "server" to refer to server hardware, operating systems, or server applications. We'll discuss each of these below.

Server Hardware

In hardware terms, a server is a computer dedicated to providing information and other resources to other computers on a network. The size of a server can range from a large room full of processors to an ordinary desktop computer. Almost any computer can act as a server. However, servers are usually larger, more powerful specialized computers that can handle resource-intensive tasks better and more efficiently than desktop computers.

The key hardware components in servers are very similar to the hardware in a regular computer. For example, a server includes one or more processors, one or more hard drives, and a variety of network and other interface ports. Your server hardware requirements will vary considerably, depending on what you want your server to do. Print sharing and file sharing aren't particularly taxing for a server, whereas hosting large databases or image libraries will require considerably more sophisticated server hardware.

Just like regular computers, servers also come in various shapes and sizes (or "form factors"):

- **Tower servers** are free-standing towers similar to desktop computer towers. Because they can't be stacked easily, tower servers usually require more floor space than other server form factors. They're often a good choice for an organization's first server, especially for smaller organizations.
- **Rack servers** are more compact, and they are designed so that multiple servers can be arranged in a mounting rack or cabinet. They are also more scalable, meaning it is relatively easy to add more servers and to connect to external storage. A rack server arrangement is most appropriate for an organization with extensive computing needs and in-house tech support.
- **Blade servers** are even more compact, allowing you to fit more servers into a smaller space. They are also designed to be more tightly integrated together than rack servers. A blade server arrangement is also most appropriate for an organization with extensive computing needs and in-house tech support.

For a detailed description of relevant server hardware components, see Dell's [Server Hardware Configuration Guide](#).

Server Operating Systems

Servers run specialized versions of operating systems. Microsoft, Apple, Linux, and others all have server versions of their operating systems:

- [Windows Server 2008](#) is considered an industry standard by many IT professionals. Windows Server includes many built-in server applications and is built to work with Office and other popular Microsoft products. [Small Business Server 2008](#), intended for smaller organizations, combines the core functionalities of Windows Server with SharePoint Server and Exchange Server.
- [Ubuntu](#) is the most popular variant of Linux for desktop computers, but it's also appealing as a server operating system because of its ease of use, performance, and security (that it's free doesn't hurt either). It includes built-in file and print server functions.
- [Mac OS X Server](#) offers many of the same features but is optimized for an office that uses Macs.

Server Applications

Server applications are software designed to run on servers. They help you perform tasks like file and printer sharing, hosting your organization's email, and performing backups.

As your network grows, you will find uses for a variety of specialized server applications. A few examples are included below.

- **File and Print Servers**

File servers and print servers are the most common types of servers. File servers allow multiple users in a network to share one or more hard drives. Administrators can configure security features to allow only certain users to access or edit particular folders and files. File servers are also useful for backups.

Print servers allow multiple computers to share printers.

The same machine may serve as both the file and print server in smaller networks. Many server operating systems include built-in file and print server functionality.

- **Backup Servers**

Centralizing backup in your organization with a server application is a good policy. With a backup server, backup can take place automatically throughout a network, and backed-up data can be readily available in case of emergency. If unwanted data loss occurs on a computer, an administrator can repair or replace that computer's hard drive and then use the backup server's copy to restore the computer's data.

- **Email and Communications Servers**

Email servers collect email and other forms of communication and distribute them to the appropriate users. Many email servers can also manage calendars, contacts, tasks, notes, and more. Some email servers include options to allow users to check email and other services from any web browser.

Communications servers, many of which can integrate with email servers, manage live communications like web conferencing, instant messaging, and voice services like calling and voicemail.

- **Database Servers**

A database is an organized collection of data similar to a spreadsheet (in that both store their data in tables). But databases are much more versatile and powerful in their ability to analyze, sort, compile, and use data in other applications or websites. Databases can serve many purposes, from tracking donations or events to compiling information from multiple sources to measuring your organization's impact.

Using a database server allows multiple users to access or edit data more easily. Database servers can also help automate the processes of collecting and publishing data. Finally, certain advanced reporting and donor management systems will require a database server.

- **Web Servers**

A web server is the server used to run a website. It stores your website's files, images, and text and "serves" that information to web browsers and web-based applications. Due to the cost of hardware and bandwidth, it isn't recommended that you host public websites from your in-house servers. Finding a third-party web hosting service is more feasible for most organizations. For an introduction to web hosting, see the Websites section later in this Guide. [A Few Good Web Hosting Providers](#) provides an in-depth explanation of how to select the right one for your organization.

Assessing Your Server Needs

The following questions can help guide your server selection process:

- How will the server fit in with your existing technology?
- Can you set up power and cabling for your server?
- What do you need the server to do? File sharing, file storage, and printing? Backup? Hosting applications, centralized databases, or CRM tools? Email hosting? Other tasks?
- How much storage space do you need? Think about how many computers you currently have in your organization, the type of files you'll be storing on your server, and any expected changes or plans for growth in the next few years.
- Which operating system do you plan to use? Every server application has specific operating system requirements, meaning the application is designed to run a specific server operating system (such as Windows Server or Linux).
- What are the system requirements of the operating system and server applications you plan to use?
- What kind of warranty and technical support is available? Options vary considerably by vendor, and often there will be multiple tiers of support available. If having any server downtime would be disastrous for your organization, invest in same-day on-site support service, if possible.

For more information on selecting a server, see PCWorld's [Server Buying Guide](#) and PCMag's article [How to Buy a Server](#).

Securing Your Server

Just as you take steps to secure individual computers in your organization, you also need to secure your servers.

- **Install antivirus software:** Your server needs antivirus protection just like your computers do. Most major antivirus software vendors offer products that are designed for use on servers.
- **Provide physical security for the server:** Place servers in a secure location such as a locked room. When not in use, lock (password protect) the server console.
- **Back up regularly:** Having a backup copy of your organization's data is crucial if your server is damaged or destroyed.
- **Improve fault tolerance:** Fault tolerance is the ability of your server to handle an unexpected hardware or software failure. Two key technologies for improving fault tolerance are a redundant array of independent disks (RAID) and an uninterruptible power supply (UPS).
 - In a RAID setup, data is stored redundantly across two or more hard disks. That way, if one disk fails, your data is still available on the other disk(s).
 - A UPS protects your server from accidental surges and power loss. Your UPS should include a cable and software to automatically shut down the server when the battery power runs low. The UPS should be able to power your equipment long enough so that the equipment will shut down normally (at least 20 minutes).

- **Install intrusion detection software and/or host auditing software:** Host auditing and intrusion detection software monitors servers for signs of unauthorized intrusion.
- **Review server logs periodically:** Your server will automatically create a log of what the server has been used to do, including things like who has accessed the server, what information was accessed, any errors that occurred, and what changes were made. Reviewing these logs can help you monitor server performance, address problems, and identify security issues.

Server Alternatives

There are alternatives to investing in a server. Although these solutions are less customizable than traditional in-house servers, their simplicity and affordability may make them right for your organization.

- **Cloud Applications**

Many server-like applications such as email and file sharing can be accomplished with cloud applications. As discussed previously, with cloud applications your organization's data, software, and other resources are hosted on servers outside the organization. You access the cloud application over the Internet via a web browser.

- **Network Attached Storage**

Network attached storage (NAS) devices allow you to add hard drive-based storage to your network without having to install and maintain a full-blown server and are available at a fraction of the cost. In a small compact package, NAS devices also offer many server-like functions such as database hosting, backup space, or printer sharing. However, with simplicity comes less flexibility; you won't be able to install any additional applications beyond the ones that come with the device.

Internet Service Basics

Internet connections can be a huge expense for your organization. So how do you make sure you're getting the right Internet service (at the right price)?

To start, you need a solid understanding of your organization's current and future technology needs. What services do you offer your staff and constituents? What are your requirements in terms of bandwidth, latency, and uptime? For that matter, what do bandwidth, latency, and uptime actually mean?

This section will introduce some key Internet service terms and help you ask the right questions when choosing an Internet Service Provider (ISP).

Learn the Basic Terms

- An **ISP** is the company that provides your organization with access to the Internet. In the U.S., the major providers of Internet access are phone companies, cable companies, and government entities. There are also smaller ISPs that rent equipment and services from larger companies.
- **Internet connection types.** The most common connection types are DSL, cable, fiber optics, and dedicated leased lines. They vary in their speed capabilities (measured in Megabits per second, or Mbps) and in cost.

- **DSL** uses traditional telephone lines, and DSL performance depends on how far you are away from your nearest telephone exchange. DSL speeds can reach 15 Mbps for downloads and 1 Mbps for uploads.
- **Cable** Internet works over standard television cable lines, and speeds may be up to 50 to 100 Mbps for downloads and 2 to 10 Mbps for uploads.
- **Fiber-optic** lines offer even better performance with download speeds of 15 to 150 Mbps and upload speeds of 5 to 35 Mbps.
- **Dedicated leased lines** are dedicated (meaning not shared) fiber-optic or copper lines you lease from an ISP. This is the most expensive but also the most reliable option because you do not share the line with anyone else, and service levels are guaranteed as part of your contract. Speeds range from 1.5 Mbps (T1 connections) to 4.5 Mbps (T3 connections).
- **Broadband** doesn't refer to one specific kind of technology. Rather, it's a catchall term for a fast Internet connection. The U.S. Federal Communications Commission (FCC) currently defines broadband as 4 Mbps for downloads and 1 Mbps for uploads. DSL, cable, fiber-optic connections, and dedicated leased lines are all capable of providing broadband-level Internet access.
- **Bandwidth and throughput** are sometimes used interchangeably, but they're not quite the same. They both refer to the amount of data that can be transferred between two points on a network in a given period of time. Bandwidth generally refers to a theoretical maximum, while throughput is a real-world, practical measurement. The distinction is relevant because ISPs will usually advertise their bandwidth, which is often higher than the throughput that you'll actually receive.
- **Uptime**, sometimes referred to as availability or responsiveness, refers to the amount of time that a network connection is functioning and usable.
- **Latency** refers to the amount of time (usually measured in milliseconds) it takes for data to travel from one location to another across a network. It is sometimes referred to as delay, because your software has to wait for data to travel back and forth across the network before it can perform a particular task.
- **IP address** is the identifier for a computer or other device. If your organization needs to host services such as web, mail, or VPN, use static IP address(es). If this is not the case, use dynamic IP addressing.

Factors to Consider When Choosing an ISP

Factors to consider when shopping for an ISP include:

- **Business versus residential.** ISPs usually distinguish between the services they offer to business users and to home users. Business-class connections provide more reliability, greater upload speeds, and other advantages important to some nonprofits. However, they'll usually cost a lot more. If your needs are limited, your organization might not need a business-grade connection.
- **Reliability and service level agreements.** Most business-class Internet connections come with assurances regarding uptime, latency, and other metrics. For example, your ISP might guarantee that 99.9 percent of the time your connection will work, and they promise to refund some of your money if they don't meet that target. These promises are usually captured in a formal document known as a Service Level Agreement

(SLA). An example of a [Service Level Agreement](#) can be found at [Speakeasy.net](#).

- **How long does the contract last?** ISPs will sometimes offer reduced rates in exchange for a long-term contract. Be cautious about any contract that lasts for more than two years. The services, prices, providers, and technologies are changing all the time. You don't want to be locked in to a long-term contract when a cheaper, faster service shows up in your community a year from now.
- **What are the terms of the contract?** Are there restrictions on what you can use your Internet connection to do? For example, some ISPs' residential service contracts expressly forbid hosting websites or other online services. There may also be caps on the amount of data you can upload and download over the course of a month.
- **Uploading versus downloading.** While you probably spend most of your time on the Internet downloading files and information, you should still pay attention to upload speeds. This is especially true if you host your own website or other online services or make frequent use of cloud-based services such as file storage and online backup. Most broadband connections marketed to home users are asymmetric. In other words, the upload speed is much lower than the download speed. Business-class broadband connections will usually provide more bandwidth for uploading than residential connections.
- **Integrated voice and data service.** It's becoming more and more common to get both voice and data services from the same vendor, over the same lines, sharing much of the same equipment. For example, you can lease a T1 line from your phone company and use it for Internet traffic and phone traffic, and a single device can handle routing and security for both services. Integrated services can be less expensive and less complicated to manage than separate voice and data services.
- **Equipment and installation costs.** Residential plans usually have low equipment and installation costs. In contrast, for some business-class Internet connections, the equipment can be hugely expensive, and the installation and setup fees will usually be much higher. You may be able to roll some of these initial costs into your monthly bill by renting equipment from your ISP, but you'll trade lower up-front costs for higher ongoing costs.
- **Redundancy.** Sooner or later, your Internet access will go down, so it's helpful to plan ahead by thinking about other ways you can access critical online resources and information in the event you lose your primary Internet connection. For example, if the cellular phone network is still up and running, you can use mobile devices to access information online even if your organization's Internet connection is down.

Understanding Your Bandwidth Requirements

So how much bandwidth do you need for your Internet connection? Well, that depends on your current usage and your future needs.

Understanding your current usage includes:

- **Knowing your users.** Think carefully about the applications and websites your staff and clients use today. What sorts of functionality do you think they'll be asking for in three years or five years?

- **Monitoring your network traffic.** How fast is demand for bandwidth growing in your organization? How much bandwidth did you use six months ago and how much are you using today? Network monitoring tools can help you track this information. [ABC: An Introduction to Network Monitoring](#) explains what network monitoring tools can do, and the Stanford Linear Accelerator Center has an [exhaustive list](#) of free and commercial solutions.

You'll also need to think about your organization's future needs.

First off, you should review your organization's technology plan or strategic plan. These documents will include information about upcoming changes that could impact your bandwidth requirements. For example, are you planning to hire more staff or do you plan to use new bandwidth-intensive technologies?

The following are some potential changes that would have a major impact on what type of connection you need:

- **Increased use of video and audio.** Video and audio files are big, and transmitting them over a network takes a lot of bandwidth. As your organization looks to engage your constituents with multimedia, sufficient bandwidth to manage large files is important.
- **Adopting cloud solutions.** As discussed previously, when you are accessing cloud services, you will require a more robust Internet connection.
- **Switching to VoIP.** VoIP, which stands for Voice over Internet Protocol, refers to the transmission of phone calls over data lines and Internet connections. If you want to use your Internet connection to carry phone calls, you'll probably need more bandwidth.

Remember: You Don't Have to Do It All on Your Own

Shopping for and assessing different Internet access plans is complicated and time-consuming. Look for ways to share the work, share best practices, and (even better) share costs.

- **Ask an expert.** Ask questions in TechSoup's [Networking Forum](#) and consult your peers in the nonprofit (and for-profit) world regarding what their organizations are using.
- **Team up.** See if you can partner with other organizations nearby to negotiate a better deal with your ISP. With increased size comes increased leverage and negotiating power. You'll also be able to share the burden of understanding and managing the different technologies.
- **Let your ISP manage the equipment.** For some broadband solutions (such as T1 lines), you can rent networking equipment (router, firewall, etc.) from your ISP and pay them to do maintenance and troubleshooting. Sometimes the managed equipment still resides in your building; in other cases, it's hosted by your ISP. Obviously, you pay more for this type of service.

Additional ISP Resources

- See PCWorld's [Guide to Choosing an ISP](#).
- To learn more about integrated data and voice solutions, see TechSoup's article [Unified Communications Options for Nonprofits](#).

→ Website Basics

In this section, we'll talk about some basic questions to ask when planning or updating your website. We'll also introduce some basic components of websites, including the domain name, web hosting, and content management systems. Finally, we'll introduce other important topics such as mobile web design, social media integration, search engine optimization, measuring your website's success, and creating accessible websites.

Planning Your Website

Knowing what kind of web presence you want, how you plan to maintain it, and how you will fund it in the long run will help you both in the technical work of building the site and in budgeting for ongoing needs. These kinds of discussions should be part of your organization's overall technology planning process, as outlined in the Baseline Standards.

A little organizational soul searching needn't be a lengthy process either, and may be as simple as sitting down to answer a few key questions:

- **What do you need a website for?** Do you simply require a place where people can find your contact info and mission statement, or do you need a site where visitors can find news, register for events, post questions, interact and network with others, or make donations? TechSoup's article [A Cooperative Approach to Web Design](#) is full of great tips for determining the purpose of your website, setting and measuring goals for your website, identifying and communicating with stakeholders, and more.
- **What resources do you have to build your site?** Very simple sites may be practically free to build and host, but more complex ones will require special skills, including programming, information architecture, web design, and editing. Do you have staff available to help plan and implement your site or will you need to rely on contractors or volunteers?
- **How will you maintain your website?** Even simple, fairly static websites require a certain degree of maintenance and oversight. What kind of staff resources can you devote to maintaining your site over the long run?
- **How will you integrate your site with existing tools?** Depending on your needs, you may want to integrate the same tools you use for constituent and membership management with your website. Be sure to check in with these vendors to make sure that you choose an online solution that meshes well with these tools to avoid costly customizations down the road.
- **How will your site incorporate your current graphic language?** Make sure you can choose a solution that brands your organization in a way that's consistent with your other printed materials.

- **Can you take steps now to plan for future needs?** No one has a crystal ball, but projecting a couple of years into the future may help you create a website with more staying power.

What You Need to Know About Websites

Even if you never need to write a single line of code for your site, arming yourself with an understanding of some basic technologies will help you every step of the way. This knowledge will help you specify what you need and ensure a common vocabulary when working with consultants and others who may help you implement your website. It will also help you understand what's happening when problems arise.

Get to Know the Basics

For an accessible introduction to the technical elements behind your website (such as HTML and Cascading Style Sheets) see the TechSoup article [How Websites Work](#).

Registering Your Domain Name

The **domain name** is a unique string of letters and numbers that identifies a site on the Internet. TechSoup's domain name, for example, is www.techsoup.org. Nonprofits and social benefit organizations usually choose domain names that end in [.org](#). While there's no rule that requires nonprofits to choose a [.org](#) domain name, it is conventional (just as educational institutions usually choose domains ending in [.edu](#), for-profit companies in [.com](#), and government agencies in [.gov](#)). You may also want to register at least the [.com](#) and [.net](#) versions of your domain name as well as the [.org](#) version to avoid having someone else registering and using a very similar domain name.

To learn how to register a domain name, see PCWorld's step-by-step guide to [registering a domain name](#).

Choosing a Web Host

A **web hosting** company (or web host) specializes in maintaining the hardware, software, and high-speed Internet connections necessary for a fast, reliable website. A good provider is one that specializes in web hosting and has all the appropriate infrastructure, security, and backup technologies in place to ensure your site stays operational.

The web host uses a *web server* to store the files that make up your organization's website and connects them to the Internet so people can see your site.

Web hosting companies typically charge customers on a monthly or annual basis. Options and costs vary considerably, but as is often the case, the trade-off for lower cost is usually a less flexible and less powerful system. The most common hosting categories are:

- **Basic shared hosting**, where your website is one of many websites hosted on a single web server, is the cheapest way to host a website. However, you may be limited in terms of what software you can install. You'll also likely have limited system memory and processing resources, so shared hosting isn't well-suited for high-traffic websites or websites with especially complicated functionality.

- **Virtual private servers** are a step up from shared hosting in terms of power and flexibility (and cost). You share server hardware with other websites, but you get your own dedicated virtual server operating system to work in.
- **Dedicated servers** are the premium option. You get a dedicated server for your website, which gives you maximum flexibility. This is the most expensive option and also requires substantial experience with server technologies.

For a detailed explanation of how web hosting works and key considerations when selecting a web host, see Idealware's [A Few Good Web Hosting Providers](#). For a current review of some small-business shared hosting options, see PCWorld's article [Which Web Host Do You Need?](#)

Using a Web Content Management System (CMS)

For a site that will grow with your nonprofit and meet the needs of multiple stakeholders, you'll probably want to invest a little time and money into adopting a web CMS. A CMS is a kind of software that you install on your web server, and it helps you create and update a website with minimal technical skills. It also allows you to more easily manage varying types of website content. CMSs also offer tools for managing site design, navigation, and user access.

A CMS certainly isn't the only tool you can use to create and maintain a website, but CMSs are a popular choice because they combine a high degree of extensibility, flexibility, and customizability for website administrators, with ease of use and simplicity for authors and content creators.

A CMS facilitates:

- **Updates by multiple users:** A CMS helps you manage multiple users and give them different access rights. So, when you're updating a page, you can be sure you're working with the most recent version, and you'll be sure two people aren't making edits at the same time. You also have more granular control over who can create, update, or remove content from your website.
- **Updates by non-technical staff:** Most modern CMSs include a WYSIWYG (what you see is what you get) editor, meaning that you can format text and add links without needing to actually write any code.
- **Managing your content efficiently:** CMSs store the site's actual content (like text and images) in a database. The CMS pulls the content out of the database automatically and displays it on the appropriate pages based on rules you set up in advance. So, for example, if you want to announce an upcoming meeting or event, adding the announcement to a bunch of individual pages would be a pain. With a CMS, you can make the change centrally to add the same announcement to multiple pages at the same time.

For much more on selecting and using a CMS, see Idealware's comprehensive guide [Comparing Open-Source Content Management Systems](#).

Going Mobile

According to some researchers, within the next few years, more people will go online via their mobile devices than via PCs. What does that mean for your organization's website? It means that you can expect an ever-increasing percentage of constituents and potential volunteers and donors to be viewing your website via a mobile device. It also means that making sure your website is mobile-friendly should be a priority in your organization's technology plan.

There's good news and bad news about making your website mobile-friendly. The good news is that your website will already display on any mobile device with a web browser. The bad news is that it probably doesn't look very good on a mobile device. Mobile devices typically have much smaller screens than PCs, so content that's easy to read on a big monitor may be very difficult to read without a lot of pinching and scrolling on a mobile device.

A lot of people also read their email via their mobile devices. So, what happens when they see your organization's email call to action and click on a link to your website? When they get to your website, will it be easy for them to donate or sign a petition or join a volunteer event using their mobile device?

You have a few options for making your website mobile-friendly: you can optimize your current website so that it looks better when viewed via a mobile device or you can create a mobile-specific website. Which approach makes the most sense depends on your organization's resources and how much of a priority mobile users are for your organization.

NTEN's article [Four Strategies for Going Mobile](#) provides a clear breakdown of various strategies.

Integrating with Your Other Technology

No matter what web-development option you select, be sure to consider any tools that will need to integrate with it. If you have any constituent databases, donation processing tools, or membership management software, for example, talk to your software vendors before committing to a web-development tool.

Incorporating Social Media

If you're using social media tools like Facebook or Twitter, these tools should be integrated with your website. This means your overall communications strategy should consider how your social media and website work together. Social media should also be integrated into the website itself. This can be as simple as installing a widget that displays your Twitter feed in a sidebar on your home page or including the ability for visitors to share your news and content via various social media tools.

TechSoup's webinar [Integrating Social Media with Your Website](#) offers best practices for coordinating across the various social media and online channels as well as practical advice for integrating social media features into your website. Social media tools are also discussed in greater detail in the Exploring Social Media Adoption section of this Guide.

Getting Noticed with Search Engine Optimization (SEO)

A beautiful, functional website design doesn't help your constituents if they can't find your website in the first place. So, if someone uses a search engine to find domestic violence shelters in your area, does your website come up in the search results? Does it come up towards the top of the first page of results? Search engine optimization (SEO) techniques can help make a findable website a reality for your organization.

What does SEO entail? Well, to start, it can be as simple as making sure you have a well-designed, technically sound, and informative website. Google, for example, has a detailed [list of guidelines](#) that will help ensure your site shows up in their search results. These guidelines include a variety of useful web design best practices, including advice about how to format and organize your website content.

For an introduction to SEO, see TechSoup Canada's [SEO Introduction](#). For a much more in-depth discussion of SEO, check out this [Beginner's Guide to Search Engine Optimization](#).

Measuring Your Success with Web Analytics

Web analytics is the way you measure, collect, analyze, and report on website usage. This, in turn, lets you understand who your audience is, how they're using your site, and what is and is not working well on your site.

Web analytics include simple statistics like visits (the number of visitors to a website or page) and page views (the number of times a page was viewed). It also includes more complicated (and more interesting) measurements like bounce rate (the percentage of visitors who leave your site after viewing only one page), how they got to your site (which link or search keyword got them there), and conversion (the number of people who did what you wanted them to do on the website, like signing up for a volunteer opportunity or making a donation).

Keep in mind that using web analytics tools means you will be gathering and storing certain kinds of information about visitors to your website. Your privacy policy should clearly state what information is being gathered and how that information will be used.

Your web hosting company may offer basic analytics software for free. [Google Analytics](#) is a more robust (and also free) option. To learn more, check out Idealware's articles [Measuring the Effectiveness of Your Online Communication](#) and [A Few Good Web Analytics Tools](#).

A Reminder about Accessibility

In their [Web Accessibility Initiative](#), the Worldwide Web Consortium (W3C) defines web accessibility as follows: "*people with disabilities can perceive, understand, navigate, and interact with the Web, and that they can contribute to the Web.*"

Making your website accessible includes basic web design best practices similar to those recommended in SEO guidelines. It also includes specific steps, like adding text descriptions of images and captioning or transcripts for audio. Your site should also be compatible with assistive technologies. To learn more, see [Web Content Accessibility Guidelines at a Glance](#).

So is your organization's website accessible? W3C's list of [Web Accessibility Evaluation Tools](#) can help get you started evaluating your site and making it more accessible.

Additional Website Resources

- For design tips, check out [5 Tips for Visually Enticing Nonprofit Websites](#).
- For a good roundup of website-coding resources, see [HTML is Easier Than It Looks](#), which includes links to a nice series of [Google-produced video tutorials](#).
- To learn more about making your website mobile-friendly, read these [mobile design strategy tips](#) and get some practical [usability guidelines for websites on mobile devices](#).

Section 4: Budgeting for Technology

All the tech know-how in the world won't help you if you are unable to fund the hardware and software you need. Your budget should contain technology costs, hardware, software, training, and support as line items.

A detailed discussion of budgeting and accounting principles is out of scope for this Guide, but a few things to keep in mind are:

- The budget should include estimated costs for *all* aspects of the technology purchases you have listed. A common mistake is to include only hardware and software purchases in the budget. Actually, a good rule of thumb is that approximately 70% of your technology spending should go to technical support and training and only 30% to technology purchases. See Total Cost of Ownership section below for additional information.
- Be sure to include staff assignments and time budgets.
- Think about your budget over the course of several years. Technology assets have a life cycle, and planning ahead lets you be prepared for the future.

→ What to Include in Your Budget

At minimum, your technology budget should include the following:

BUDGET ITEMS	BUDGETED AMOUNT
Hardware	
Software	
Support and maintenance contracts	
Cloud or other hosted services (website domain name and hosting, ASPs, email)	
Services (consultants, advisors)	
Ongoing costs	
Training	
Staffing	

→ Understanding Total Cost of Ownership (TCO)

There are additional costs for most things beyond what you pay up-front. Technology is no exception. When budgeting for technology costs, you need to consider total cost of ownership (TCO), which is the full cost of purchasing a piece of technology, not just the up-front cost.

For example, when you're setting out to buy a new computer, the latest prices on a vendor's website represent only a percentage of the true, long-term cost of that computer. Installation, maintenance, training, tech support, and replacement parts are a few of the hidden costs of technology.

Some things to think about with TCO:

- **Staff Support:** How much time will your staff spend supporting and maintaining the new technology?
- **Vendor Fees:** Will you be paying any ongoing support or licensing fees to the vendor?
- **Staff Training:** Any time you replace a major productivity tool such as your office productivity suite, staff will usually need some formal or informal training.
- **Bandwidth Costs:** Will you need a faster Internet connection to handle the new technology?
- **Hardware Costs:** Does the software you're considering require new hardware?
- **Infrastructure Costs:** Computers need electricity, and they have needs in terms of temperature and humidity. Will there be additional infrastructure requirements to support your new technology?
- **Technology Replacement:** How long will it be before you need to replace this technology and how much will it cost?
- **Additional Supplies:** Think about things like paper, ink, and toner for printers and copiers.

→ Understanding Return on Investment (ROI)

On the other hand, some technology acquisitions and upgrades will make your staff more productive or improve the services you offer. This is called return on investment (ROI) or total value of ownership (TVO), and you should consider it alongside the TCO.

Considering the value or return on your technology investment is also helpful when developing your technology strategy.

Some things to think about for ROI:

- **Services Provided:** It's hard to measure the impact that a new technology will have on the services your organization provides, but it's one of the most important considerations.
- **Staff Productivity:** Will staff be able to do their jobs faster with the new system you're considering? How many extra steps and unnecessary workarounds does your staff use to deal with the quirks and limitations of your current technology? For example, if you're tracking your income and expenses using a clunky, 10-year-old piece of software, could you save time in the long run by upgrading to a newer version?
- **Staff Support:** If a new technology is more reliable and user-friendly than the solution you have in place, your staff will spend less time fixing problems.
- **Staff Training:** User-friendly technology reduces (but does NOT eliminate) the need for staff training.

This return on your technology investment doesn't necessarily offset costs from a budgeting perspective, but thinking about ROI does help you understand and articulate the value technology may provide.

→ Additional Resources

- NTEN's [Nonprofit IT Staffing and Spending Report](#) can help you understand what other nonprofit organizations are spending on technology.
- The Toolkit in the Appendix has more information.

Standard 2: Secure Network and Data



This stage will help you identify how you are currently keeping your information secure and how to protect it on a regular basis.

Part of this process includes documenting your current support maintenance processes, including job descriptions, staff assignments and communication/reporting systems, and current data and privacy protection procedures. This section also introduces some basic security and privacy concepts to help you better protect your organization and its data.

Section 1: Documenting Support and Maintenance Systems

→ Who Takes Care of Technology in Your Organization?

Technology isn't something you can just buy and then forget about. Ongoing maintenance, support, resources, and management are essential, or the technology will degenerate. This includes things like:

- IT management (budgeting, planning, decision making)
- Network troubleshooting
- Desktop troubleshooting
- Database administration
- Backup administration (running backups, performing restores)
- Website updates
- Email account changes
- Software license tracking

Who is responsible for performing these tasks in your organization? Who do you call when something stops working? Do you have internal support available, or do you rely on external support? It's OK if you don't have someone assigned to perform all these tasks at this stage. We'll look at improving support for your organization's technology in Standard 3.

To get started documenting these roles, see *Technology Responsibilities Worksheet* in the Appendix.

→ Technology Job Descriptions

Most organizations rely on a mixture of internal and external support for their technology.

It is important to include technology support responsibilities in your staff job descriptions. This is especially important for the "accidental techie," who helps manage technology for your organization, but whose primary job responsibilities are not tech-related. Adding technology support to the accidental techie's job description recognizes that this is an important part of their role, just as their regular non-technical work is, and it allows them to allocate time in their work day for tech support tasks. The key is to identify these roles and not let them just be taken on ad hoc.

Some typical internal roles may include:

- An **Accidental Techie** is a staff member with basic technology skills but whose primary responsibilities are not technology-related. Often an accidental techie participates with management to make technology decisions rather than taking sole responsibility for those decisions.
- An **Information Technology (IT) Manager** is a staff member with an IT support background whose primary job function includes IT support for the organization. Their role includes overseeing and supervising all work completed by the network/computer support staff (and vendors), as well as ensuring that essential IT tasks and activities are completed (example: backups, network security updates, etc.). They are responsible for forwarding IT support and infrastructure questions and requests to appropriate channels, so they can make key decisions regarding inventory purchases and infrastructure needs. They also provide recommendations to managers, directors and board members regarding future IT strategies and resources that will support the organization's mission.
- An **Information Systems Director** oversees all IT staff. While the IT Manager makes technology recommendations (upgrades, software installation, documenting networks, etc.), it is the Information Systems Director who makes the final decisions on the plans, policies, and strategies.

For sample *IT Manager*, *Information Systems Director*, and *Accidental Techie* job descriptions, refer to the Appendix.

→ How Do You Communicate About Technology?

What is your organization's process for communicating about technology? When something goes wrong, who do you call? When you want to improve something or install new software, is there a process in place for making that suggestion? Are technology issues and their resolution documented in any way?

Your process can be as simple as writing down who should be contacted for particular technology issues (as recommended earlier in this section) and keeping notes on what issues occurred and how they were resolved. Or, for larger organizations with more complex technology to support, it can include implementing help-desk issue tracking software to help manage your technology support and maintenance processes.



For small organizations, see the Tech Support Contact Information Worksheet and Tech Support Tracking Template included in the Appendix.

For larger organizations, or organizations with more complex technology support needs, see TechSoup's article [Choosing Help-Desk Management Software](#).

Section 2: Collecting and Reporting on Data

As we digitize our operations more, we collect more data. Data can be anything from the amount of electricity your shelter uses to standard inputs like how much money you spend to familiar outputs like how many clients you've served in a month.

As our ability to collect more data increases, we must also learn how to turn data into meaningful information. This section will introduce some basic data collection and reporting concepts and provide tips on how to become a more data-driven organization.

→ Storing and Using Data

Your data can be, and probably is, everywhere in every format possible. You have paper files from years ago, videos you took in VHS format, or computer files in a backup drive format that's not even supported anymore.

If you're a shelter, you'll be keeping track of how many clients come through your doors in a month. Do you just keep paper copies of intake forms? Do you have an intern enter that data into a spreadsheet? Do you then enter that information into a client management database? All three methods are collecting data, but they differ in how useful and accessible they are for future analysis.

Data that you gather on a paper form may be the most secure and straightforward. It will always be there when you need it. You make notes on it for future reference, and it can be safely kept somewhere. But unless it is digitized, you would not be able to quickly determine trends in a population, like demographics, nor would you be able to tell quickly how often a person sought help or whether they have related needs. It almost always requires extra work to make sense of it all. Unless you've made sufficient paper copies and placed them in multiple locations, you can also lose everything in a natural disaster. You can, however, make infinite copies of digital data.

Slightly better than paper files would be the numerous spreadsheets you keep, which do give some insight into the work you do. For budgeting purposes, a spreadsheet allows you to view and plan for funding, but it's an inadequate tool to understand clients. A good rule of thumb is that if you don't need to perform calculations on the data, it probably doesn't belong in a spreadsheet.

On the other hand, a spreadsheet is a great way to determine data relationships. Using our earlier example, you can use a spreadsheet to find out the number of clients served in a shelter per shelter staff and use that as a metric to compare performance between shelters. Without the proper data collected, you would not be able to gauge your organization's performance. Having data in an analyzable form allows you to see gaps in your programming or ways you can be more efficient in your operations.

Moreover, it is often worthwhile to figure out trends beyond just those required. For example, by charting not just the number of requests or visits seen but discrete clients (as opposed to returning clients), you may be more inclined to see if that is due to population growth or reduced services from local governmental agencies or just greater awareness due to a new campaign. These are the kinds of reporting that decision-makers and funders want to see as you look to deepen your impact.

Outcomes like greater awareness and community cooperation can't always be captured in a single metric. Tools like databases or CRM systems help organizations manage the relationship and interactions for all of your stakeholders. It can also indicate the scale and amount of activity you have within your network of supporters, which you are ultimately trying to grow beyond just numbers and donations.

→ Common Tools to Collect and Analyze Data

In a nonprofit, there are many tools available for you to collect and analyze data. Here's an overview of some commonly used tools:

- **Database:** A database stores information as records, kind of like a digital index card file. It can contain as much information as you would like in each record. While the complexity, functionality, and level of specificity of each database program can differ, the underlying premise of storing data as records remains the same.
- **CRM:** A CRM system is a database application that is focused on viewing and understanding the activities and actions of a donor, client, or organization. By tracking the phone calls, emails, and meetings with individuals, users can understand and proactively interact with constituents.
- **Business intelligence software:** This type of software allows you to analyze data from different sources, including some data from online sources, for an overall view of the organization. It is best used when you already have data collected and organized and are ready to organize it for sharing and analysis.

→ Next Steps to Be More Data-driven

We have discussed how to be more data-driven and the reasons to think about your data differently. But you have limited resources, and your staff is overwhelmed, so what can you do? Here are some concrete steps we recommend you take:

1. **Cleaning house:** In order for you to take stock of what you have, you must start thinking about your data as an asset to your organization. It is not just a by-product of your work, but rather the foundation upon which you can do more for your constituents more effectively. That means that you need to figure out what data needs to move out of paper forms and convoluted spreadsheets into databases and CRMs. Your resident accidental techie or IT person should be able to guide you through the process, as they are probably also managing your backups of that data.
2. **Understand your data:** Once all your data is digestible by software, you should think about (in consultation with them) what information is important to your stakeholders. Is it financial efficiency, scope of impact, or a return on investment? Understanding these perspectives will help you figure out what the missing information is that can take your fundraising or impact analysis to a different level.
3. **Make the information compelling:** Data tells stories and gives snapshots of your organization. The spectrum of complexity in displaying your data is very wide, but using imagery and visuals will make that data compelling and easier to understand. Reporting functionality is built into most data-related software. It could be as straightforward as a bar chart showing raw figures, or a more abstract "infographic" that shows a variety of facts and figures.

→ Advanced Data Usage

Once you have mastered the fundamentals of data collection and analysis, there are other possibilities for more advanced usage. Here are some examples:

- **Dashboarding:** A dashboard, like the one in a vehicle, displays information, often from many different sources, in an easy-to-read format. These are usually top-level performance indicators, and many CRMs offer customizable dashboard modules for different departments and members. For example, development staff can focus on funding-related data in charts and graphs, while operations can focus on staffing and service levels.
- **Social analytics:** As more data is generated from online interactions, the data from all your Facebook comments and Twitter retweets can be aggregated to understand reach and popular topics. Coupled with more traditional metrics and website visits and email open rates, social analytics can be a power tool to understand your online presence and ways to strengthen it.
- **Location and mapping:** Nonprofits are beginning to combine location and mapping data to get a view of their reach for both internal and external use. For example, using location and mapping tools, you could represent your client base using their zip codes then overlay school districts with the addresses to figure out where you want to launch a youth education campaign.

Section 3: Security and Privacy Basics

Your organization handles sensitive and confidential information, so securing it is a high priority. In this section, we will help you identify and evaluate how you are currently keeping your information secure and how to protect it on a regular basis. This will include guidance on:

- Why data privacy and security matter
- Documenting data privacy policies and procedures
- Best practices to help keep data secure

→ Why Data Privacy and Security Matter

Most organizations keep some sensitive personal information in their files: names, addresses, phone numbers, social security numbers, or records of how clients use your organization's services.

Your staff, volunteers, donors, and, most importantly, those who use your services trust that this personal information is safe with you. Unfortunately, stealing and selling personal information is a lucrative illegal business. Organizations involved in domestic violence prevention and support are especially concerned with protecting their clients, staff, and volunteers' information. Information security breaches can also have major legal and financial ramifications for an organization.

Regulatory Compliance

Beyond protecting your clients, staff, volunteers, and donors, sometimes organizations are legally obligated to take additional steps to protect their data, including encrypting certain files and communications.

Your specific organization may have additional legal obligations, but the main regulations nonprofit organizations usually need to worry about are:

- **Health Services:** Any organization that transmits electronic billing information to any health insurance provider, Medicare, or Medicaid is covered by the Health Insurance Portability and Accountability Act (HIPAA) and must meet certain security standards. Additionally, any organization that stores or transmits user login or patient information may need to be compliant with the [HIPAA Security Standard](#), even if it is not technically a covered entity. See Idealware's [In Search of HIPAA-Compliant Software](#) on selecting HIPAA-compliant software and visit the official [HIPAA website](#) at the Department of Health and Human Services for more information.
- **Storing or Processing Payment Information:** Organizations that store or process payment information such as donor credit card numbers need to be familiar with Payment Card Industry Data Security Standard (PCI DSS). For more information on PCI DSS and compliance, visit the [PCI SSC website](#).
- **Mandatory Notification of Privacy Breaches:** Many states, including California, have laws requiring you to provide notification when personal data is stolen, lost, or accidentally disclosed.

The good news is that basic security and privacy policies and procedures can go a long way toward helping protect your organization's data and the people your organization serves. Though these safeguards are not always legal requirements, they can help ensure your organization's mission is not compromised by security breaches.

→ Understanding Security Threats

There are many ways that security and privacy can be compromised, and not all of them have a technology solution. Your users (staff, volunteers, visitors, and clients) are also an important part of keeping your organization secure.

For example, if you look at the top ten technology threats facing most organizations, you can see that many of them have very little to do with technology.

THREAT	MOSTLY A USER ISSUE	MOSTLY A TECHNOLOGY ISSUE
10. Cyber espionage (mostly affects governments)		X
9. Cloud computing		X
8. Known issues without a fix (these are called "zero day exploits")		X
7. Social engineering, called "phishing"	X	
6. Social networking	X	
5. Mobile devices (mostly due to theft)	X	
4. Employee carelessness	X	
3. Exploited vulnerabilities		X
2. Malicious insiders	X	
1. Viruses, spyware, and other malware		X

Source: [Net Security's Top 10 Information Security Threats](#)

We will provide guidance on addressing many of these technology concerns, but you should always keep in mind that training your people is also a critical part of keeping your organization's technology secure.

→ Documenting Data Privacy Policies and Procedures

The first step in protecting data privacy is understanding how you are currently collecting, storing, and transmitting data. Just like doing a technology inventory helps you develop your organization's technology strategy, a privacy inventory will help you develop your organization's data privacy and security strategy.

If you already have a data privacy policy in place, that's great! The policy itself and your data privacy procedures should be periodically reviewed and updated. The questions below can help you with this periodic review.

Understand What Data Is Sensitive

Personally identifiable information is particularly sensitive. This would include:

- Name, address, phone numbers, email addresses
- Social Security number
- Credit card and banking/financial information
- Health and medical records

Keep in mind every organization is different, so your organization may be gathering other sensitive information in addition to the above.

Identify What Kind of Data You Collect and How It Is Collected

- Who provides sensitive personal information? Those who use your services, your staff, volunteers, and donors, obviously, but there may be other sources for personal information.
- How do you get that information? Through email, your website, in person, through the mail? Are there other ways you gather information?

What Do You Do with the Data You Collect?

- This is where you answer the "why" question. Why do you collect that data? How is it used? Is that data necessary to perform particular tasks or provide services?
- How long do you store that data?

Where Is the Data Stored and Who Can Access It?

- Where do you keep the information you collect? Computers, servers, databases, and paper filing systems are an obvious place to start, but also think about mobile devices, portable storage or "thumbnail" drives, external hard drives, off-site storage, employees' home computers, digital copiers, and other devices.
- Who has access to the data? Who has permission to access it? Do they need access to that data? Could they access it even without permission? Don't just think about people inside your organization. Also consider vendors, contractors, and other service providers who may have access to your organization's data.

How Do You Transmit or Share Data?

- How is personal information shared or transmitted? Think about how you transmit data: via phone, email, instant messaging, file-sharing or collaboration tools, portable storage devices, or over your organization's network.
- How do you handle personal information requests?
- Are you subject to any mandatory reporting requirements?

What Processes and Technologies Do You Currently Have in Place to Keep Your Data Secure?

- Are computers, files, servers, and storage devices kept in locked areas?
- Do you perform regularly scheduled data backups? Where are your backups stored? How secure is that storage?
- Do you have a firewall in place?
- Do you use up-to-date antivirus and anti-spyware software?
- What is your password policy? How often are passwords changed?
- Do you use encryption to secure your website, network, email, or stored data?
- Do you train your staff in how to protect personal information and how to use data securely?
- What other processes do you have in place?

How Do You Dispose of Data When It Is No Longer Needed?

- Are there any mandatory data retention policies your organization is subject to? If so, how long must that data be stored? How do you store it?
- After you no longer need data, how do you dispose of it?
- Are paper files shredded or otherwise destroyed?
- How is data wiped from old electronic devices, including portable storage drives, external hard drives, laptops, computers, mobile devices, and digital copiers?

Assess Your Security

- What are the risks you face from a security breach and what are the possible consequences of that breach?
- What would it take to address those risks?
- What resources and processes do you currently have to address these risks?
- What other resources and processes do you need to put in place?

Your Organization's Privacy and Security Policy

Your organization's privacy policy and procedures should:

- Specify the type of client, staff, and/or other data that is gathered, how this data should be handled, who should have access to it, and (in general terms) how that data will be secured.
- Identify any exceptions to the policy, such as mandatory reporting requirements.
- Address what data must be retained, how long the data should be retained, how it should be transmitted and stored, and how it should be deleted or destroyed at the end of the retention period.
- Clearly describe what steps your organization will take in the event of a data security breach.

Privacy and Security Policy Resources

- The SANS Institute is a great resource for [free sample policies](#)
- TechSoup also gathered [sample policies and advice](#) from a variety of organizations

→ Best Practices to Help Keep Data Secure

Now that you know what kind of information your organization is gathering, how it is stored and used, and who is accessing it, it's time to start thinking about any gaps in your data privacy and security procedures and how to address them. This section will provide tips and best practices to help you keep personal information secure.

Tip 1. Limit the Data Your Organization Stores.

The best way to prevent personal data security breaches is not to store that data in the first place. If you don't have a legitimate need for sensitive personal information, do not collect it. You can, for example, almost completely outsource credit card payment processing. That way, your organization is not responsible for gathering, storing, or protecting credit card information.

You should also be especially cautious about storing data on laptops, mobile devices (smartphones or tablets), and on portable storage devices. These smaller devices are easy to lose and easy to steal.

If you do need personal information, only store it as long as it is required to perform the required task (or as long as you are legally required to retain it). When the data is no longer needed, dispose of it properly.

Tip 2. Limit Access to Sensitive Data.

Access to sensitive personal information should be strictly limited to those who need that information. Access should be controlled both physically and electronically, and access should be reviewed periodically.

Tip 3. Implement Basic Technology Safeguards.

At a minimum, organizations should have or plan to implement the following:

- Regular scheduled backups
- A firewall
- A password policy
- Antivirus and anti-spyware software
- Encryption tools, if appropriate

We'll briefly cover each of these technologies and describe some tools that may be appropriate for your organization.

Regularly Scheduled Backups

California organizations in earthquake-prone areas need to think about what would happen to their data if disaster strikes. However, regular backups are vital insurance against other kinds of data-loss scenarios as well, including device loss, theft, or simple human error. Every organization should implement regularly scheduled backup procedures.

Your organization's backup plan should cover:

- What's being backed up
- Where it's being backed up
- How the backup data will be secured
- How often backups will occur
- Who's in charge of performing backups
- Who's in charge of monitoring the success of these backups

There are different approaches to backing up. Local backup means your computer copies your data to a separate hard drive or other storage media. Local backups should be stored separately from the system you have backed up. In remote backup, your computer automatically sends your data to a remote off-site center at specified intervals.

Either approach (or both) may be appropriate for your organization. Your backup strategy will depend, in part, on the size of your organization's network. Though manual backups can be effective for very small networks or home offices, whenever possible use a dedicated backup tool. A dedicated tool will make scheduling backups easier. Properly configured, an automated system is more reliable and easier to manage. It also allows for easier data recovery when it is needed.

Another thing to keep in mind is that if you live in an area that's susceptible to natural disasters, you may not want to trust local backup alone. It's possible that a disaster could claim both your primary and backup drives, even if you keep the backup drive at a different location in the same city.

When setting up a backup system, pay particular attention to security. Your backup hard drive or tape will contain all your organization's vital information. Be sure that this media is properly protected, both on-site and off-site. You can password protect and encrypt

your backup data archive as well.

Backup Recommendations

	SIZE OF NETWORK		
	VERY SMALL (1-3 Computers)	SMALL (2-10 Computers, No Server)	LARGE (10+ Computers and/or Server)
Hardware	CD-R or other media	External hard drives or tape	Dedicated backup server
Software	Manual copy or Windows Backup	Dedicated backup software	
Frequency/ Schedule	At least weekly	At least weekly and store backup hard drive off site	Daily backup and store weekly version off site

Recommended Tools for Backup

- Online (remote) backup: Mozy.com and Carbonite.com
- Local (onsite) backup:

Windows and Mac operating systems both have built-in backup tools. Backup works slightly differently depending on which version of Windows you are using. Windows 7 information is available [here](#). Mac's backup tool is called [Time Machine](#).

If you have a DVD burner on your computer, it may also include backup software.
- Network-attached storage (NAS) solutions will usually include built-in backup solutions

Firewalls

A firewall is another critical component of keeping your organization's data secure. Any computer system with Internet access needs to shield itself from unauthorized access using some form of firewall. A firewall is basically a gate between the computers in your organization and the outside world. It monitors the information that flows into and out of your organization to ensure that no unauthorized network traffic occurs.

A firewall uses rules that define what information should come into your network and what information is allowed to leave your network: "good" traffic is allowed to go through, "bad" or suspicious traffic is blocked.

There are two kinds of firewalls. A software firewall is software you install on a computer. It can be standalone software you install separately, an integrated part of your computer's operating system, or part of a comprehensive security suite that also includes antivirus and anti-malware protection and other features. A hardware firewall is a device that monitors and protects your computer network. Your organization may use a software firewall, a hardware firewall, or a combination of both.

Some good firewalls to consider are:

- [Windows Firewall](#) is included as part of the Windows 7 operating system.
- [Zone Alarm](#) is a free downloadable software firewall for individual and nonprofit use. [Comodo](#) also offers a free software firewall.
- [Norton Internet Security](#) (available through TechSoup) offers comprehensive firewall, antivirus/anti-spyware, and other protection.
- TechSoup currently offers a variety of [Cisco networking hardware](#), including security appliances, to qualified nonprofits.

A Password Policy

All electronic devices used to store personal information should be secured with a password. Your organization should also develop a password policy to help your staff understand how to create and use passwords effectively.

Your organization's password policy should include:

- General guidelines for password security, including guidance on creating strong passwords.
- Expiration: How often passwords should be changed.
- Reporting and Enforcement: How your organization will handle breaches in password security.

Some general guidelines for password security include:

- Do not share passwords with anyone. All passwords should be treated as sensitive, confidential information.
- Passwords should not be written down.
- Don't reveal passwords via telephone, email, chat, or other online communication.
- Log off before leaving a computer unattended.
- Change temporary and default passwords immediately. Passwords like "admin" and "password" should also be changed to a stronger password immediately.

Strong passwords are:

- **Long:** Passwords should be eight or more characters.
- **Complex:** Should include a combination of uppercase and lowercase letters, numbers, and non-alphanumeric characters such as * \$ & # ^ %) ? (@.
- **Hard to Guess:** Avoid dictionary words, your name, your account name, the name of your organization, the names of family, pets, friends, co-workers, movie or TV characters, etc. Also avoid using birthdays and other personal information such as addresses and phone numbers, and avoid word or number patterns like aaabbb, qwerty, 321123.

- **Changed Frequently:** Ideally, passwords should be changed every 3-6 months.
- **Vary Between Accounts:** Use different passwords for work and personal accounts. Use different passwords at work for accessing different accounts, where possible.

One easy way to create a strong password is to start with a phrase you know and will remember and develop your password based on that phrase.

WHAT TO DO	EXAMPLE
Start with a phrase you will remember, maybe a song title, affirmation, or favorite quotation	"Be the change you want to see in the world."
Create a password using the first letter of each word in your chosen phrase	btcywtsitw
Add capital letters and special characters	Btcyw2sitw!

For added password security:

- Require that certain passwords are changed periodically for critical systems or especially sensitive data (this can often be automated).
- New passwords should not be based on a small change to an existing password. For example, change from Btcyw2sitw! to Btcyw2sitw!2.
- Automatically lock an account after a specified number of failed password attempts.
- Some devices have a setting that allows you to automatically wipe all data from the device after too many incorrect password attempts.

Antivirus and Anti-spyware Software

Malware is a catchall term for threats such as viruses, spyware, adware, and other software installed on a computer or mobile device, usually without your consent or knowledge. Malware can get into your system in various ways, including (but by no means limited to) infected email attachments, removable storage devices like portable thumbnail drives, downloaded software (including mobile apps), and links in email, social media or other websites, or instant messages

Malware can destroy or alter data, spy on your activities, steal private information, or harness your computer to send spam messages or perform illegal activities. Keep in mind, a "smart" mobile device is basically a small handheld computer, so smartphones and tablets are also vulnerable to malware, just like computers are.

Because of malware's potential to corrupt, alter, or steal data, we strongly recommend that you equip every computer in your organization with a comprehensive antivirus program and a separate anti-spyware program.

You also need to make sure your software is up-to-date. Both antivirus and anti-spyware software monitor your computer for potential threats, and mostly they identify suspicious software based on a list of known threats, called "definitions." Definitions are updated when new threats appear, and usually you can download these updates automatically. Up-to-date definitions are what allow your antivirus and anti-spyware software to recognize and stop new threats.

The specific tools you choose will depend in part on the size of your organization:

- Very small organizations with only a few computers should install individual antivirus and anti-spyware software on every computer.
- Organizations with 10-20 computers should consider using a security suite. A suite allows you to administer software centrally, rather than dealing with each computer separately.
- Organizations with more than 20 computers should consider enterprise-level tools. Enterprise-level tools also allow centralized administration of definition updates and other tasks, as well as providing additional security tools appropriate for bigger organizations.

There are many low-cost or free options available:

- [Norton Internet Security](#) is a popular antivirus and anti-spyware solution available as a TechSoup donation. [Norton 360](#), also available through TechSoup, includes antivirus and anti-spyware features, and other computer maintenance tools.
- [Symantec Endpoint Protection](#) is suitable for larger organizations and is available through TechSoup donations.
- [Microsoft Security Essentials](#) is a free antivirus and anti-malware download for Windows users, most suitable for a small office.
- [McAfee](#) and [Kaspersky Labs](#) also provide good, reasonably priced antivirus solutions, and both offer special nonprofit organization pricing.
- Using a separate anti-spyware tool will help protect against a broader range of threats. Each company maintains its own threat list, and no company's list is complete. [MalwareBytes](#) is a good free tool.

A Note on Spam

For most nonprofit organizations, email spam is a nuisance, flooding your inboxes with irrelevant advertising. But spam emails can also infect computers with malware by encouraging users to visit malware-containing websites or download malicious files.

To spare your organization hassle (and potential security breaches) due to spam, it is highly recommended that you have anti-spam filters in place. Look for an email provider that offers spam filtering. If your organization operates an email server of its own, set up a spam filter on the server. There are also built-in spam filtering options available in Microsoft Outlook. Also make sure your staff and volunteers are familiar with the basics for using email safely and securely.

For more on preventing spam, see TechSoup's article [Things You Can Do to Prevent Spam](#).

Encryption Tools (If appropriate)

Encryption is a way to convert information (such as phone calls, email messages, or the data on a computer) into a coded format that can't be read or understood by an unauthorized person. Only an authorized person who has the key to unencrypt (or "decrypt") the information can convert it back to its original, understandable format.

Encryption technology can help protect the information and identities of the people your organization serves. Organizations that store health information and credit card information may also be legally required to implement additional encryption safeguards.

Encryption technologies can:

- Create a secure connection so that information transmitted to and from your website is protected.
- Protect the contents of a computer, portable storage device, or off-site backup.
- Keep your wireless network secure.
- Create a Virtual Private Network (VPN), a secure connection between a computer outside your organization's network and the network itself. This allows you to access information stored inside your organization, even when you are off site.

Any organization that acquires, stores, or transmits sensitive or personal information should consider implementing additional encryption safeguards. Below are some areas to consider using encryption tools, the relevant minimum standard you should be looking for, and some useful tools.

WHAT YOU NEED TO SECURE	STANDARD	SECURITY AND ENCRYPTION TOOLS
Your website	TLS/SSL	Comodo , Verisign , and Geotrust products
External or internal drive, or individual files	AES-128 or -256	<p>TrueCrypt is free, open-source disk encryption software for both PCs and Macs.</p> <p>Windows Vista and 7 include BitLocker, which lets you encrypt individual folders or an entire drive.</p> <p>Mac OS X includes FileVault, a tool for encrypting your Mac's hard drive (earlier versions allow you to encrypt only the home folder).</p> <p>Espionage can also be used to encrypt data on Macs.</p>
Wireless network	WPA2 (Wi-Fi protected access) with 802.1X	All wireless networking equipment supports some form of encryption.
VPN (remote access to data from outside your organization)	TLS/SSL or IPsec	<p>Citrix GoToMyPC (available through TechSoup) and LogMeIn are good tools for smaller organizations with just a few users needing remote access.</p> <p>Organizations with more employees may want to investigate a more comprehensive VPN solution. See Additional Resources for more information on remote access solutions.</p>

Tip 4. Pay Attention to Physical Security.

Physical security is another critical part of your overall technology security, and it should be included in your privacy procedures.

- Paper documents, files, storage media like CDs and backup tapes, and external hard drives should be secured.
- Servers and other key network components should be kept in a locked cabinet or room. Make sure wireless access points are hidden or kept in a secure location. If not secured, someone could easily come by and reset the device to its original factory defaults, rendering your wireless network insecure.
- Laptop computers should be locked down at all times with a cable lock.

- Everyone should log off or shut down the computer before leaving it unattended.
- Password-protected screen savers can be set up to automatically lock after a computer is unattended for a specified time. Most computer operating systems include this feature.

Tip 5. Know What You Will Do if a Breach Occurs.

What should employees do if a device is lost or stolen, a password breach occurs, or private information is shared inappropriately?

- If an account or password compromise is suspected, this should be reported to a designated person immediately.
- Passwords should also be changed immediately if there is suspicion an account may have been compromised.
- Understand your legal and ethical obligations for reporting security breaches.

Tip 6. Train Staff.

Make sure policies and procedures are clearly communicated to new staff and retrain existing staff periodically. Make sure everyone understands what their responsibilities are, how to deal with security and privacy issues, who to contact, and what the consequences are for violating your organization's policies in this area.

Tip 7. Inform Your Constituents.

Given the particularly strong privacy and security concerns for domestic violence organizations, you may want to take additional steps to help protect those who use your services.

- Teach them how to browse the Internet safely, including using private browsing features, clearing their browser history and browser cache, and clearing toolbar and search history.
- Teach them how to protect their email.
- Offer clients and constituents multiple methods for contacting you.

Once you have a written policy that describes how you will handle private information, you should also communicate that information to those who are using your services. A few ways you can do this include:

- Post it on your website's home page.
- Post it on a prominent sign in your office.
- Give people a copy of the policy when they use your services.

Tip 8. Use Social Media Wisely.

Social media can be an effective outreach, advocacy, and engagement tool, but it can also raise some security and privacy concerns. Here are a few tips for keeping safe when using social media.

- Social Media is based on personal exposure. The core business model of social media companies is to learn who you are, who you know and share this with other companies. This is not the place to have a private conversation!
- Be aware of social media privacy policies and changes to those policies. Regularly check your personal settings to understand what you share and what you don't share and to keep up on the frequent changes by these companies (this is especially true for Facebook, but holds true for other sites as well).
- Use social media for the right reasons: marketing, build a constituency around your services; advocacy, build support for your causes; education, share current news, research, and other stories that explain areas of what you focus on.

Tools Your Organization Can Use Right Now!

The following are some inexpensive or free tools your organization may want to look at:

- Backup online now: www.mozy.com
- Remove viruses now: www.housecall.trendmicro.com
- Remove viruses ongoing: www.techsoup.org/stock
- Firewall and privacy: www.auditmypc.com
- Audit your PC: www.open-audit.org
- Wipe all data from old PCs: www.dban.org

Additional Security and Privacy Resources

- TechSoup's [Security Forum](#).
- Security Essentials Guides: The Federal Trade Commission has an excellent plain language [interactive online guide](#) to small business security essentials. The [U.S. Chamber of Commerce](#) and the [U.S. Department of Commerce](#) also offer good security essentials guides.
- [Stop Think Connect](#): quick, easy tips for safe emailing, web surfing, and other healthy and secure computing basics.
- Antivirus and Anti-Spyware: Idealware's [antivirus protection article](#) and TechSoup's [Removing Spyware, Viruses, and Malware](#) are specifically for nonprofits.
- Networking and Remote Access: [Demystifying Remote Access: Part 1](#) and [Demystifying Remote Access: Part 2](#), PCWorld's tips for [Wireless Network Security](#).

- Backup: TechSoup articles [Local Backup for Your Organization](#) and [Remote Backup for Your Organization](#) and Idealware's [A Few Good Tools for Online Data Backup](#).
- Disaster Planning: [The Resilient Organization: A Guide for Disaster Planning and Recovery](#) and the TechSoup webinar archive [Disaster Planning: Backup, Backup, Backup!](#)
- Software Reviews: [PCWorld](#) and [CNET](#) are good general sources for software reviews.

Standard 3: Implement Network Support and Maintenance



After completing the tasks associated with Standard 2, your organization will have a clear picture of what you need to secure and what your top priorities are. During this next stage, you will begin to implement those support and maintenance tasks and activities, including basic recommended security tools and best practices.

Standard 3 also includes improving your organization's technology support. This section includes recommendations for developing and improving internal staff support and knowledge, as well as tips for working with external support, such as volunteers, consultants, and technology support providers.

Section 1: Securing Your Assets

While documenting and assessing your organization's technology in Standard 1 and reviewing security and privacy policies and procedures in Standard 2, you probably found some things that weren't working as well as they should be. Now is the time to correct these problems.

Securing your organization's data should be among your highest priorities. Use the checklist below to make sure you complete the recommended steps.

→ Secure Technology Assets Checklist

By completing these tasks, your organization will have a better protected and operational computing system.

SECURE TECHNOLOGY ASSETS CHECKLIST	COMPLETED
Organization has basic security and privacy policies in place, including data privacy, acceptable use, and privacy policies.	<input type="checkbox"/>
Organization has minimum standards for user passwords in place, including a password policy, and has implemented tools and procedures to ensure compliance with password policy.	<input type="checkbox"/>
There is a process in place for regularly managing user accounts, including removing old user accounts.	<input type="checkbox"/>
Physical security is sufficient to protect technology assets.	<input type="checkbox"/>
An appropriate network security appliance, such as a secure router, is installed and managed.	<input type="checkbox"/>
Antivirus and anti-malware protection is installed and regularly updated.	<input type="checkbox"/>
Anti-spam solution is installed at the provider, server, or individual workstation, as appropriate.	<input type="checkbox"/>
Encryption technologies are used to secure organization's data and communications, as appropriate.	<input type="checkbox"/>

Section 2: Maintaining and Supporting Your Systems

The guidelines and recommendations in this section will assist you with user support and staff training to help you maintain your organization's technology. It will also include suggestions for working with external support resources such as volunteers, consultants, or professional tech support providers. You can also use the checklist below to make sure you've completed the recommended steps.

Improve Technology Support Checklist

By completing these tasks, your organization will improve its internal tech support capabilities.

IMPROVE TECHNOLOGY SUPPORT CHECKLIST	COMPLETED
Staff receive training and periodic reminders of organizational technology policies such as password, acceptable use, and privacy policies.	<input type="checkbox"/>
Staff is aware of and utilizes basic healthy and secure computing best practices.	<input type="checkbox"/>
Job-specific technology training needs are identified, and steps are taken to meet those needs.	<input type="checkbox"/>
Systems maintenance tasks are scheduled and performed on a regular basis, including server and network monitoring, software patch management, and backup.	<input type="checkbox"/>
Responsibility for technology support tasks is clearly identified, and staff is informed of and follow the procedure for contacting technical support resources.	<input type="checkbox"/>
Process exists for documenting technology issues, support requests, and the resolution of any issues.	<input type="checkbox"/>
For internal resources, tech support responsibilities are included in their job descriptions.	<input type="checkbox"/>

→ User Support

Any organization that uses computers needs to have some form of user support. Lack of this first-level support will almost always result in significant costs in terms of staff time and data loss.

There are two main approaches to providing desktop user support: *internal support* resources, such as an IT manager or accidental techie, or *external support* from a volunteer, consultant, or professional tech support provider.

→ Internal Support

Any organization that makes significant use of computers should have some level of internal IT knowledge. Below are tips for improving your organization's internal tech support capabilities through staffing and training.

Staffing for Internal Support

A staff member with basic computer support training can solve many of the day-to-day problems encountered by desktop users. They should be able to:

- Help you implement desktop software.
- Provide basic desktop troubleshooting skills and networking skills.
- Document problems and solutions using something as simple as a paper log or as complicated as an automated help-desk issue tracking system.
- Coordinate working with external support resources

Smaller organizations may find their needs are best met by selecting a staff member who has basic IT skills but whose primary responsibilities are not IT-related, the accidental techie. Remember, even though tech support isn't their main job, their tech support responsibilities should be formalized and included in their job description.

When identifying or hiring staff who will have technology responsibilities, keep in mind:

- Not everyone is suited for (or interested in) a technology role.
- They don't need to be a hard-core techie, but you definitely want someone who is interested in technology. You want someone who doesn't mind digging into technical issues and gets some enjoyment out of problem solving.
- They must have good communication skills. A key function of a technical person is explaining technical issues to non-technical people and understanding non-technical people's computer hardware or software questions. Rather than look for someone to address all the technical issues that might arise, try to find someone who can listen and clearly explain technical issues to everyone.
- You should also identify a person who will be responsible for understanding and planning for your organization's long-term strategic technology needs. This person would be in charge of planning and budgeting for technology investments.
- Larger organizations or organizations with significant IT investments should have a qualified IT manager on staff who can handle both the basic help-desk functions and manage higher-level system resources such as servers and network equipment.

Training Staff

The best technology in the world benefit your organization unless your staff has the skills and knowledge they need to use the systems. Make sure that resources have been set aside to cover the costs of staff training.

There are various ways to approach technology skills training, from formal classroom lessons to informal one-to-one knowledge transfer.

Any staff member who uses a computer for daily work should have some basic skills in:

- Using the operating system
- Navigating the web
- Safe computing
- Common productivity tasks (such as Microsoft Word and Microsoft Excel)

[New Horizons](#) is a well-known national provider of technology skills training, and there are likely local organizations that provide similar services. Your local library, community college, or adult education centers probably also offer technology training. Self-directed training courses are available online through programs like Microsoft's [Software Assurance](#), which is available as part of TechSoup's Microsoft donation program.

As mentioned previously, TechSoup's articles [Learning About Technology Online](#) and [Learning About Technology Offline](#) include a variety of other resources for learning about technology.

- **Training for Specific Procedures**

Your organization probably has unique processes such as how data is organized on your file server, or you may use specialized software. Ideally, you will already have documented how these systems work as part of Standard 1. This documentation can be the basis for training your staff on specific procedures.

- **Training in Specialized Software**

If your organization uses specialized software, you will need to develop a process to train new users on these systems. You can provide *external training* on these applications, such as vendor workshops, or *internal training*, such as one-on-one training given by a knowledgeable user (called a "super-user").

If you can't afford to send all your staff to external training, we recommend that you choose one user to become the trainer. If it is available, this user should go through a "train the trainer" version of the software training, so that he or she can then train other staff members. It is important in these circumstances to send someone who has the aptitude to be a good trainer as well as a solid understanding of how the system is used in your organization.

- **Role-Based Training**

Often someone in your organization will have unique knowledge of the systems involved in his or her job role. In this case, they should be able to transfer this knowledge to other staff, either through accurate documentation or through job shadowing or one-on-one training.

→ External Support

Most organizations need to have access to high-level technology expertise when problems occur that cannot be handled by their own staff. Many organizations would rather not spend resources on internal tech support but instead look to external support providers on an as-needed basis.

Depending on an organization's specific IT needs, volunteers with good technical skills can be an adequate resource, though they may be unable to provide immediate emergency support. Consultants are another option. Professional support organizations can usually offer fast and effective support, though at a higher cost.

Working with Volunteers and Consultants

Unpaid volunteers or consultants that are paid on an as-needed or project basis are an attractive option for budget-conscious organizations. However, there are some key issues you must consider when you are ready to enlist non-staff to help you.

Best Practices for Working With Volunteers

Aside from the basic fact that volunteers are not paid monetarily for their time and consultants are not on the payroll as employees, both these groups are different from staff in that they will have varying levels of experience with your line of work.

Here are some tips that we find particularly important when working with technical volunteers:

- **Understand what they want to accomplish:** It is likely that more skilled volunteers would prefer more complex tasks that are perceived as more impactful, but that may not always be the case. Therefore, it's important to understand beforehand what your organization and the volunteer would like to get out of one another. For example, are they here to learn more about the issues you tackle? Do they prefer more social or public-facing activities? Knowing this beforehand allows you to match the project to the best candidate.
- **Properly define project scope:** Volunteers cannot be expected to provide support indefinitely. Therefore, project scope needs to be determined in the beginning and not allowed to "creep" or expand beyond that. Tech projects should have defined deliverables and milestones. Reining in the project scope in the beginning and throughout the project will ensure that you and your volunteers' time are well spent.
- **Insist on adequate documentation:** All organizations should properly document their technology projects, but it's particularly important to do so for volunteer projects. This starts with a clear project plan, status updates, and final reports on completed and outstanding items. Unlike staff, volunteers may not be on site to answer your questions mid-project, and, worst case scenario, a volunteer may have to leave mid-project to tend to other priorities. Sufficient documentation ensures that the project, or what's left of it, can be picked up by another volunteer or member easily.
- **Be mindful of experience:** You may be working with an experienced volunteer from the corporate sector or a newly graduated but inexperienced college student or a recent retiree wishing to contribute. Using what you have learned from this Guide, you should be able to define the project in a way that is helpful to all parties.

Best Practices for Working With Consultants

Working with consultants requires a similar level of thoughtful planning and oversight. The benefit of working with consultants is that their work for you is clearly defined in a contract or statement of work. They are likely to better understand the nuances of the sector and what constraints you may have. They are also held to a higher standard in terms of service delivery and guarantees. Lastly, consultants are more likely to be

obligated to provide assistance beyond the project.

Still, they are not like the accidental techie or part-time system administrator, so you should expect the following when working with them:

- **Consultants cannot decide for you:** Consultants are knowledgeable about the subject matter and can help make recommendations based on your situation, but they ultimately don't know as much about your organization as you do. When selecting a consultant, ensure that you have done enough research to be able to give them the information they need.
- **Be resolute about your budget and time constraints:** No nonprofit technology setup is perfect, and more often than not it is a mix of old and new, out-of-the-box and customized setups. If a consultant is telling you to overhaul your system for more than you can afford or promoting a solution that is beyond your capacity or capability to support, then make sure they are doing it with good reason. Educating yourself, via this Guide and other resources, is the best way to know what's most necessary for your organization.
- **Get clarity on future support provided:** You'll need to be able to support the solution after the consultant is gone. Unlike volunteers, where the expectation is that the time commitment is limited, consultants are usually expected to provide some form of support after the project is completed. This should be negotiated beforehand as part of the contract, and you should make sure that it's adequate to the needs of your organization.

Knowledge transfer and interaction with existing staff

We recommend that you identify a tech-savvy employee to be a point person for the project and for communicating with any volunteers and consultants. Having someone who is more versed in the technology situation of the organization acting as a liaison will facilitate the conversations between volunteers/consultants and stakeholders. It's also good to have a single main point of contact for your volunteers or consultants. Having multiple staff members give different or conflicting messages is one good way to scuttle a project. There may also be staff members who wish to learn more about technology. If they become that liaison, this could be a great learning opportunity for them as well.

Working with an External Support Company

In addition to consultants, there are many companies that offer tech support. If you decide that this model is a good fit for your organization, there are a few things you need to do to make sure you select the right company and the right level of support.

Tips for Choosing a Support Company

- **Know what technology you have.** You need to be able to clearly describe the technology setup they will be supporting.
- **Know what support you already have in place.** What can you support using existing internal resources? Do you already have support in place for particular software, hardware, or other technology? For example, does your accounting software include phone support?

- **Know what you want them to support.** Based on your current technology and internal support resources, clearly define which portion of your technology setup the support company will be responsible for.
- **Understand your requirements.** Do you expect phone, email, or on-site support? What response times do you expect? At what times of day (or night) should support be available? Do you want the support provider to have remote access to fix problems?
- **Choose carefully.** Check with your peers and see who they have used. Ask for references from each company you are considering.
- **Consider confidentiality and security.** This company may have access to sensitive data. What security procedures do they have in place? What guarantees do they offer regarding confidentiality?
- **Review the contract.** Make sure you understand both the services they are providing and your responsibilities as their client. See Lasa's article [What to Expect from an IT Support Contract](#) for more detail on what your contract may include.

→ Additional Resources

- Get the most out of your volunteers with TechSoup's downloadable handbook [Working with Technical Volunteers: A Manual for NPOs](#).
- Ask questions in the TechSoup [Volunteers and Technology Forum](#).
- Find people interested in microvolunteering (very- short-term volunteer opportunities) at [Sparked: the microvolunteering network](#).
- For working with consultants, see the TechSoup articles [When to Use Consultants](#), [Choosing the Right Consultant](#), and [Managing a Consultant](#).

Standard 4: Update and Sustain Network Assets and Infrastructure



Now that your organizational systems are more secure and efficient and your computing resources are being supported and maintained, it's time to update your computing systems and infrastructure. If you have completed the tasks and documentation identified in Standards 1-3, you now have a clearer picture of what essential hardware and software should be purchased and/or donated to your organization. During this stage, you will also tackle the "what if" of a disaster and develop a plan to protect your organization and its assets in the event of an emergency.

Section 1: Update Network

Based on the documentation and strategy developed in previous standards, begin updating hardware, software, infrastructure, and other technology assets in order of priority. This may include tasks like:

- **Hardware upgrades:** Do you have computers that are more than 4 years old? If so, consider replacing them or upgrading their hardware.
- **Software investments:** Invest in software based on your tech strategy. Strive for standardization as much as possible.
- **Networking improvements:** Identify which critical pieces, when upgraded, would have the most return. Is it an old hub that only permits speeds of 10 Mbps? Or a wireless router that needs resetting every now and then? Or maybe a switch that has maxed out its connections? Do you need a better way for staff to access resources on your network when they are outside of the office?
- **Server investments:** If your organization is not using a server (and could benefit from one), explore server options. If you are using a server, make sure you are using current versions of the server operating system and server applications and that you are following server security best practices.
- **Website enhancements:** Does your website need an overhaul? What kind of back-end systems are you using to create and maintain your website? Can you benefit from implementing search engine optimization techniques? Are you evaluating your website using web analytics tools? Are you compliant with accessibility recommendations?

Section 2: Disaster Planning

How prepared is your organization for a disaster scenario? If you lost all of the paper files in your office, how much time would it take to recreate all of that information? How about all of the data on a single laptop? All of your computers? What happens to your work when the phone or Internet connection goes down?

Disasters are often the times that communities most rely on the nonprofit sector. When a disaster strikes, it's important for your nonprofit to be able to resume operations quickly and spend those key hours and days providing needed services in the community. If you haven't taken adequate steps to prepare your organization, you may risk being unavailable when your constituents need you. Poor planning is a liability not only to your nonprofit but also to the people who rely on it.

Fortunately, the key elements of disaster planning – backup, security, documentation, and clear policies – *are also elements of good IT policy*. In other words, the same precautions that will make your organization ready for a natural or human-made disaster can also help your day-to-day operations run more smoothly and efficiently. For this reason, we hope that this Guide will not only prepare you for a crisis but deepen your nonprofit's impact in times of health too.

This section will briefly cover the key elements of disaster planning. For much more information, download TechSoup's free guide [The Resilient Organization: A Guide for Disaster Planning and Recovery](#).

→ Documentation

The first and most important step you can take to prevent or minimize the impact of a disaster is to document your technology infrastructure thoroughly.

Although you can reconstruct things like passwords, warranty information, and tech support information by looking through old receipts and emails, it's better to take the time compiling that info *before* a disaster than during or after one. Having clear, up-to-date documentation of your tech infrastructure in the hands of the people who need it will be hugely instrumental in helping your organization resume operations in a time of crisis.

The process of documenting your tech infrastructure was already thoroughly outlined in the section on Standard 1: Establish Strategy, Policies, and Documentation. For disaster preparation purposes, you'll also want to document contact information, with home and mobile phone numbers for all staff, board members, and volunteers.

→ Unified Communications

Unified communications (UC) refers to a large family of technologies and organizational practices that simplify and integrate multiple forms of communications like phone conversations, email, video and web conferencing, instant messaging, voicemail, fax, and SMS messages.

The central idea behind UC is that if an employee can access and reply to a message using whatever device is convenient at the moment (regardless of what sort of device the message was generated on), there will be less lag time between replies, and the organization will be able to communicate more effectively internally and externally.

In a disaster scenario, communications are essential. Given that your office and communications infrastructure may have been damaged or destroyed in a disaster, it's essential that fast communication not require employees' physical presence in the office. If staff and volunteers can easily access their voicemail and email from a home computer or other device, there will be less lag time between communications. UC technologies can facilitate this kind of flexibility.

For more information, see TechSoup's article [Unified Communications Options for Nonprofits](#).

And if a UC strategy doesn't make sense for your organization at this time, at minimum you should have a backup communication plan.

→ Backup

In Standard 1, we already discussed the importance of backing up your data. The importance of regular, thorough backups is even more apparent in a disaster situation.

In choosing whether to rely on remote or local backup (or both!), think about the conditions in which your nonprofit works and how you're likely to be impacted by a disaster.

For example, one nonprofit staff member whose organization was hit by Hurricane Ike reminded us that if you're storing your backups in the same city as your office computers, there's a danger that one catastrophe will destroy both, "Consider your entire city a potential point of failure!"

For many nonprofits, online backup services are a great option, because they'll still be available even if your entire office is destroyed or inaccessible. But if you're working in a remote area, loss of Internet connectivity will render your online backups worthless.

Is Cloud Computing an Alternative to Regular Backups?

Later in this Guide, we'll discuss the ways in which cloud computing can be an inexpensive, easy-to-implement alternative to traditional software.

Are cloud tools as secure as running Microsoft Office and Outlook on your own computer? No, and they're not appropriate for storing highly sensitive information. But cloud computing services are arguably more impervious to disaster than other technology solutions.

There are a few additional considerations for cloud services in a disaster planning context:

- Which data will be most crucial in a disaster situation? Is the cloud the best place to store that data? While Google or Microsoft or other cloud providers probably won't be impacted by a local disaster, that will be of little use to you if you don't have the computers or Internet service to access it.

- How will you access the data? Be sure that you can download and back up your data in a universal format.

→ Human-Made Disasters and Accidents

The measures we've discussed thus far will prepare you for most natural disasters, but what about smaller disasters and accidents? There's no way to prevent every accident, but some minor preparations can minimize their impact.

Protect Critical Organization Logins

A clear and consistently enforced password policy is a key component of protecting your organization and its data against human error.

End-of-Employment Policy

Have a policy and procedures in place for when your organization's relationship with an employee ends and make this policy available to any employees who would like to see it.

These measures do not denote mistrust of the former employee. An end-of-employment policy provides for the smooth, professional transition that all workers deserve.

Here are some examples of the sorts of things this policy should include:

- Change any passwords that the employee had access to, including passwords for any of the organization's social networking accounts. If applicable, have the employee make a list of any accounts and passwords he set up on behalf of the organization.
- Back up the former employee's computer. Wipe all data from the hard drive before giving it to another employee.
- Archive the contents of the former employee's email (don't delete it). Forward their email address to the former employee's manager.
- Keep a list of up-to-date email addresses for former employees. This is useful for two reasons. First, it allows you to forward any personal messages an employee might receive at his old email address. Second, you might discover in a disaster that the employee forgot to document a crucial piece of information.

→ Disaster Planning Checklist

Here's a quick checklist to keep track of your progress in implementing the strategies covered in this Guide. Not every item on the checklist applies to every organization. As you work through the disaster-planning process, be sure to document new technologies and strategies that you implement and keep staff informed of new procedures and policies.

For each section, you can refer to the chapter in parentheses of TechSoup's [The Resilient Organization](#) for more information.

Communications (Chapter 1)

- Implement unified communications systems or adopt a backup communications plan
- Create a backup web presence

Documentation (Chapter 2)

- Document all critical systems and processes
- Store physical hard copies of documentation safely and securely
- Store documentation on an encrypted flash drive
- Back up documentation online

Remote and Local Backup (Chapter 3)

- Choose and implement a backup strategy
- Document your backup strategy and train staff members in backup and retrieval
- Back up data not included in backup strategy (e.g., website, paper records, etc.)
- Routinely check backups

Privacy and Encryption (Chapter 4)

- Assess security needs for all of your organization's data
- Encrypt all critical or sensitive data
- Use secure logins for donor and constituent databases
- Check compliance with HIPAA or other applicable standards

Human-Made Disasters and Accidents (Chapter 5)

- Enact a policy for critical logins
- Develop an end-of-employment policy and make it available to employees

→ Conclusion: Becoming Flexible by Default

Ultimately, disaster planning isn't just about disasters. It's about running a more flexible and prepared nonprofit. The precautions that will help your nonprofit recover in a time of disaster are the same precautions that help your nonprofit flourish in times of health.

Right now, you may have a database that includes only your donors, while your clients are in paper files, and your volunteers are in a spreadsheet on your volunteer manager's laptop. Some of your project data might be available in the cloud, while the rest is on your office file server, accessible in the office or through your slow and difficult-to-use VPN server.

When thinking about disaster preparedness (or just your organization's IT strategy), think about ways you can make your organization more flexible by addressing these kinds of issues. What if you adopted the mantra "flexible by default" at your organization? That is, what if you made it a goal that *whenever possible* you and your staff could access your work from anywhere using any computer or other device?

That level of flexibility may be impossible in some instances – either for privacy reasons or technology limitations – but if you made it a goal to build a flexible infrastructure, your organization would be better positioned to serve your community in a time of disaster. More importantly, you'd be better positioned to adapt quickly to *any* change in your community.

Section 3: Revise Your Technology Budget

The final task in this section is reviewing and revising your technology budget based on what you've already learned and tasks you've already accomplished. You should consider:

- Any changes to your organization's strategy, mission, or priorities since the budget was originally created
- Any changes to your current budget and funding situation since the budget was originally created
- Future projects based on your organization's technology strategy and plan
- Replacing or upgrading your technology assets due to expected systems obsolescence (such as aged hardware or out-of-date software)
- Meeting your organization's long-term support needs

Remember, your technology budget should address the following over a multi-year timeframe:

- Hardware
- Software
- Support and maintenance contracts
- Cloud or other hosted services
- Services (consultants, advisors)
- Ongoing costs
- Training
- Staffing

Standard 5: Incorporate Cloud & Social Media Asset



During this phase we encourage you to explore some technologies, resources, and options available to organization through cloud computing. We also advocate that you explore social media options and assess their potential for enhancing and supporting your mission. Finally, we also offer guidance on collecting and reporting on organization-wide data.

Section 1: Cloud Computing for Nonprofits

Cloud computing is gaining popularity day by day. Some organizations have been quick to move into the cloud, citing cost savings, convenience, flexibility, and environmental impact. Others have taken a more cautious tack, questioning the cloud's security and the reliability of newer cloud providers. Many nonprofits fall somewhere in between, test-driving various cloud-based tools for one-off projects before gradually moving more business processes into the cloud.

This section of the Guide is designed to help you understand what the cloud is all about and to support you in investigating whether cloud solutions are right for your nonprofit. We'll introduce some basic cloud computing terminology, outline some of the advantages and disadvantages to cloud computing, and suggest a few cloud-based solutions your organization might want to look into.

→ What is Cloud Computing?

The term "cloud computing" refers to a wide variety of Internet-based computing services. The difference between cloud-based and traditional software is that when you access the cloud, your desktop or laptop isn't the thing doing the actual computing. The computing happens in a large datacenter outside your organization, and you simply see the results of it on your own screen. Most cloud computing services are accessed through a web browser like Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome; therefore, they don't require users to have sophisticated computers that can run specialized software.

Cloud computing usually refers to a cloud alternative to something that organizations would traditionally manage in-house or "on premises". For example, a webmail service is an entirely cloud-based alternative to hosting your own email server. A cloud-based constituent relationship management (CRM) system is an alternative to running a donor database in your office.

→ Basic Types of Cloud Computing

Cloud computing is commonly broken down into three main layers. The names and definitions of these layers vary a little bit from one source to the next, but they boil down to *infrastructure as a service*, *platform as a service*, and *software as a service*. The distinctions among the three have to do with how much control the customer has over the cloud's functionality.

If your organization doesn't write or customize its own software, then your interest in cloud computing will mostly be in software as a service (SaaS), but it's still useful to understand the other options.

- **Infrastructure as a Service (IaaS)** is the foundation or bottom layer of cloud computing and includes services like storage, backup, and security. An oft-cited example is Amazon Web Services, which includes database, storage, virtual private servers, and support services that are available on demand by the hour or megabyte. Many SaaS applications rely on Amazon Web Services or other IaaS providers.
- **Platform as a Service (PaaS)** is the next level of the cloud. The vendors of PaaS services provide a certain framework and basic set of functions that customers can customize and use to develop their own applications. Examples of PaaS services include Google App Engine, Force.com, and Microsoft Azure.
- **Software as a Service (SaaS)** basically refers to any Internet-based application (software) or service. Some SaaS applications are highly customizable and you may even need a consultant to help you set them up, but they generally don't require specialized knowledge for day-to-day operation and maintenance. Examples of SaaS include Microsoft Office Web Apps, Google Apps, Salesforce, and Microsoft Dynamics CRM, all of which we'll explore in more detail below.

→ Advantages and Drawbacks of Cloud Computing

Advantages

As you move more business-critical applications into the cloud, you'll likely find that you don't need to upgrade computers as regularly, and many employees can make do without higher-end computers. That's because *the actual computing isn't happening on the computer*. A \$200 netbook can access your Salesforce and Google Apps accounts just as quickly as a \$2000 premium laptop can. Similarly, you may find that a cloud computing infrastructure requires a smaller IT staff than a traditional IT setup does, since your organization won't be the one managing the software anymore.

Cloud computing solutions are also generally greener than traditional IT because they require less in-office IT equipment. While huge datacenters require a lot of electricity, it's still a lot less than the thousands of office-grade computers it would take to perform the same big tasks. Large cloud computing providers can also optimize their datacenters for energy efficiency much more precisely than manufacturers of desktops and laptops can.

Finally, software as a service can act as a great simplifier for many organizations. If you have staff working off-site, they can access their work just as easily at home as they can in the office, with no need to set up a virtual private network (VPN). What's more, cloud tools can make it easier to collaborate with allies from outside the organization. If you're planning an event with staff from another nonprofit, for example, it's easy to create a Basecamp project where everyone can see each other's work. It's often much more difficult – and risky – to give outsiders access to your VPN.

Drawbacks

Security and availability are the main concerns that most people have about relying on cloud-based services.

You've probably heard a few high-profile reports of security breaches in cloud-based services. When thinking about cloud security, you should also have a realistic sense of your current technology situation. Fears about the cloud are sometimes based on a utopian vision of an organization's current situation. Odds are, your security isn't bulletproof, you don't have 100% systems uptime, and you may not have staff resources dedicated to IT management. In the cloud, security and management are in the hands of "trained, dedicated experts."

Although you should certainly think about the implications of a breach in your organizational data, you should also consider that in both cloud-based and self-hosted software, most security breaches are attributable to human error.

Ultimately, as one tech support representative for Microsoft Office Web Apps summed up the situation: "Security has been taken seriously in the development of [Office Web Apps] but we live in an era where major banks, corporations, the White House, and even the FBI have had their security breached by hackers. Decisions on security ... have to be taken by users at a personal level."

Cloud computing is a new and quickly-changing field, and there's always the danger that a new company might go out of business or radically change its service. A sudden change in service might not be too detrimental if you were only using the application for a one-off project, but it could be disastrous if you were using it for your entire donor database. When evaluating cloud providers, find out what options you have for backing up and extracting your data. The best services allow you to download your data in a standard, non-proprietary format.

Finally, you will become more dependent on a good Internet connection if you rely on the cloud. As more mission-critical work is done on the Internet, organizations will need much more bandwidth and will need to assure that Internet connectivity has few, if any, failures. If consistent Internet access, connection speed, or bandwidth are problems for your organization, cloud solutions may not be right for you at this time.

→ Types of Cloud Applications for Nonprofits

General Office Software

Google Docs is one of the most well-known cloud computing services, offering the ability to create and collaborate on simple documents, spreadsheets, and presentations over the Internet.

Zoho Docs is one of a handful of services offering similar functionality. Microsoft Office Web Apps is another, but Office Web Apps bridges the divide between the desktop and the cloud, letting Web Apps users and standard Microsoft Office users share documents and collaborate with each other.

Popular examples: Google Docs, Zoho Docs, Office Web Apps

More information: [Comparing Online vs. Traditional Office Software](#); [What Your Organization Should Know About Office 2010](#)

Email and Scheduling

Through Google's service Google Apps, Google can host the email for your web domain. Your staff can access its organizational email using the same look-and-feel as Google's Gmail service, but you retain administrative controls over every account in the domain. Staff can also use the service to book conference rooms and send each other appointment requests.

Google Apps is free to U.S. 501(c)(3) nonprofits with fewer than 3000 employees. For more information, see [Google Apps' nonprofit page](#).

Popular examples: Google Apps

More information: [Email in the Cloud: A Google Apps Case Study](#); [Google Apps 101](#)

CRM

CRM databases are among the most popular cloud-based tools for nonprofits. Unlike many traditional CRMs, most cloud CRM systems operate on a simple, per-user pricing model. This makes it easier, and likely less expensive, to change the number of users who can access the database as your needs change.

Depending on how your organization is structured and who needs access to your CRM, you may find keeping your CRM in the cloud to be less of a hassle. If your nonprofit has multiple branches throughout a city, then cloud CRM can be a way to collect all of the branches' shared relationships in one place. Some organizations find that simply getting donors, volunteers, institutional funders, and beneficiaries into a single database is a key first step toward improving and streamlining business processes.

Eligible nonprofits can purchase Dynamics CRM Online at \$9.99/user/month, with a five-user minimum.

Popular examples: Salesforce, Microsoft Dynamics CRM Online, Zoho CRM, CiviCRM, SugarCRM

More information: [CRM in the Cloud: Right for Your Organization?](#)

Project Management

Some of the most exciting recent developments in cloud computing have been in the realm of project management tools. These tools serve as a shared, online workspace for collaborators on a project. Employees can post updates on their progress and share the most recent versions of documents. Supervisors and project managers can set deadlines for specific deliverables, and the project-management tool can automatically send reminders to the people responsible for meeting those deadlines. Cloud-based project management tools are usually very easy to use and offer an extremely low barrier of entry to collaboration, which makes them a great fit for organizations that frequently engage with volunteers or ally organizations.

Popular examples: Basecamp, Huddle, Zoho Projects

More information: [Six Views of Project-Management Software](#); [Can Cloud Computing Change Organizational Boundaries?](#)

→ A Few Tips for Going Into the Cloud

- **Transition incrementally.** You don't have to jump in with both feet. If you want to just dip your toe in, think about trying a cloud tool that can help address a currently ineffective or challenging process. Good candidates for this kind of experiment include project management, collaboration tools and online publishing.
- **Don't focus on tools first.** Focus on your processes and workflows, then select the tools that will help you do your work better.
- **Plan for divorce:** Think of your vendor agreements as pre-nups. Make sure you can get your data back out of the cloud.
- **Overcommunicate, overcommunicate, overcommunicate.** Engage staff at all levels before, during and after your transition to the cloud. Calm their fears, stress the benefits, and clarify how this technology will better help you serve your mission.
- **Re-evaluate periodically.** Because the cloud is changing constantly, you can't just evaluate cloud solutions once. An issue that's a deal breaker for you today may be fixed six months from now, and more cloud tools are coming all the time. So, even if you're not quite ready for the cloud right now, you may find a good cloud solution at a later time.

→ Learn More

TechSoup's [Cloud Computing Worldwide](#) campaign gathers up information, resources, and nonprofit case studies about cloud computing.

Section 2: Social Media Practices for DV Organizations

Social media can be used effectively by DV organizations to increase awareness about the good works they do, build communities in support of their organization or cause, connect with like-minded organizations, and educate and inform those that may need their services.

→ Using Social Media Safely

Social media does raise some security and privacy concerns, especially for DV organizations. These security and privacy concerns do not mean you should avoid using social media. It simply means DV organizations need to have a clear understanding of what social media is best-suited to do and have clear policies in place to guide how staff and volunteers use social media on behalf of your organization.

You should also educate yourself and your staff, volunteers, and clients about using social media safely and securely. The below resources were created for DV organizations by DV organizations that have experimented with and used social media:

- National Network to End Domestic Violence: Social Networking & Privacy Tips for Domestic & Sexual Violence Programs:
http://nnedv.org/docs/SafetyNet/OVW/NNEDV_SocialNetworkingTips.pdf
- Health Is Social: Domestic Violence and Social Media:
<http://healthissocial.com/domestic-violence/domestic-violence-and-social-media/>
- National Network to End Domestic Violence's Technology Safety page:
<http://nnedv.org/resources/safetynetdocs.html>

→ Developing a Social Media Strategy

Your approach to using social media should be centered on your mission, just as your approach to any other technology should be. A mission-centered approach will help guide your messaging, interactions, and online community building.

The following outlines five basic steps to developing and executing a social media strategy:

1. **Define your objective(s):** Social media is used by social benefit organizations to support cause awareness, fundraising, volunteer recruitment, and advocacy. It is tempting to strive for all these, but if you are just getting started, it is best to focus on one. Over time, your strategy will likely evolve, and you can use that time to revisit your goals.

2. **Assign it:** You should manage social media much as your organization does other communications tasks, by making it a formal part of someone’s job responsibilities. It is tempting to hand this task off to a volunteer, but volunteers sometimes move on, which is why it is best to assign this task to someone within your organization. Volunteers can play a meaningful role in your social media activities, but they should do so under the guidance of the person charged with managing social media for your organization.
3. **Listen and observe:** Get a sense for what other organizations are doing and what conversations are happening around the issue of domestic violence. Understand where your organization fits into the social media landscape so you are best prepared to enter the conversation. Online interactions do not require the same tone as is normally used in official external messaging and, in fact, resonate more because they are imbued with a human touch. Organizations that are successful with social media understand that it requires many of the same skills that make for a good conversation in person.
4. **Build it:** Decide what platform is right for you to begin embracing social media and establish a presence within that platform. Just as you picked one or two achievable goals, you should be similarly selective when choosing your social media channels. Social media platforms such as Facebook and Twitter have their own unique sets of rules and are better for reaching certain demographic groups. Learn the differences and determine which presents the greatest opportunity for your organization. For more on the more popular social media platforms, how much time is required, advice on content, etc., consult [TechSoup’s Nonprofit Social Media 101 wiki](#) and Idealware’s [Nonprofit Social Media Decision Guide](#).
5. **Measure and readjust:** Develop benchmarks to gauge whether you are meeting your stated goals. You can track things such as if social media results in more hits to your website or what percentage of overall donations is coming in from online sources. Not meeting your goals does not constitute failure, but it may often require a readjustment of your strategy. A simple change like better messaging or making your call to action simpler is often all it takes.

→ Developing a Social Media Policy

A social media policy will help your staff, board, volunteers, and clients understand what place social media plays within your organization. In addition, a social media policy will provide guidance as to what role your organization’s stakeholders can have in support of your organization using social media.

An effective social media policy is grounded in an organization’s culture and respects the autonomy of your stakeholders. Social media policies should not simply be a list of “do’s and don’ts” – instead, they should empower your organization’s supporters. Your supporters should feel empowered to join the conversation and be engaged online community members.

If you've never crafted a social media policy, it is helpful to take look at those of other social benefit organizations. [NetSquared](#) and [NTEN](#) have tips for developing a social media policy with links to examples on their sites:

- [NetSquared: Think Tank Round-Up: Writing An Effective Social Media Policy](#)
- [NTEN: Tips for Writing Your First Social Media Policy](#)
- TechSoup also has [Social Media Guidelines](#) that can serve as an example.

Implementing a policy might first require social media training for your organization. Use your strategy as a guide to developing an educational program for internal stakeholders. (If you are interested in using videos to explain social media, consult the "[Overview](#)" section of the [TechSoup Nonprofit Social Media 101 Wiki](#).)

Some organizations have [concerns around social media use in the workplace itself](#) and whether or not it is appropriate for employees to use social media during work hours. There are arguments on both sides, and you may want to be clear where you stand regarding your own policy.

→ Additional Resources

Below are links to the social media profiles of national organizations worth following and learning from.

- [National Coalition Against Domestic Violence](#)
Facebook: <https://www.facebook.com/SupportNCADV>
Twitter: <http://twitter.com/NCADV>
- [National Network to End Domestic Violence](#)
Facebook: <http://www.facebook.com/pages/The-National-Network-to-End-Domestic-Violence/398757490729>
Twitter: <http://twitter.com/nnedv>

Conclusion

The goal of these Baseline Standards is to provide guidance and resources on some of the most important aspects of IT systems management. Ultimately, though, technology is important because of what it allows your organization to do: fulfill your mission and make a difference in your community. By going through the Standards step-by-step, we believe your organization will be better able to plan for, implement, and sustain the technologies that help you do this important work.

Contributors

We would like to thank Christine Tran of the Blue Shield Foundation for providing guidance and support in the development of these resources for the DV community. Her expertise and unique perspective contributed greatly to the effort.

The following TechSoup staff members were the primary contributors to creating this Guide:

- Mary Duffy
- Ariel Gilbert-Knight
- Elliot Harmon
- Kevin Lo
- Michael DeLong
- Susan Tenby

We would also like to thank the following:

- Eric Leland, a Partner at [Five Paths](#), who also contributed to this effort
- Paula Doubleday, at [Paula Doubleday Design, Inc](#) for the graphic and instructional design
- Kathy Chandiok, at ASAP for copy editing services
- Dianne Mahan, LCSW

In addition, portions of this Guide and the Toolkit originally appeared in other places, including:

- The [TechSoup for Libraries](#) publication, *[The Joy of Computing: Planning for Success](#)*, funded by the Bill and Melinda Gates Foundation and created by TechSoup staff and hundreds of librarians who offered their time and expertise to the effort.
- TechSoup's [Healthy and Secure Computing Workbook](#)
- A [nonprofit technology planning article series](#) created by Tierney Smith and Jane Zhang of [TechSoup Canada](#).
- TechSoup's articles
 - [A Nonprofit's Guide to Building Simple, Low-Cost Websites](#) by Chris Peters
 - [A Field Guide to Servers](#) by Elliot Harmon and Adam Chapman
 - [An Introduction to Transport Layer Security](#) by Carlos Bergfeld
 - [Cloud Basics for Nonprofits and Libraries](#) by Jim Lynch
 - [Do I Need a Server?](#) by Henry Kumagai
 - [How Websites Work](#) by Elliot Harmon
 - [Investing in Computers? 7 Questions to Consider](#) by Ariel Gilbert-Knight
 - [Making Sense of Software Licensing](#) by Chris Peters
 - [Removing Spyware, Viruses and Other Malware](#) by Zac Mutrux



- [Tips for Designing \(or Redesigning\) a Nonprofit Web Site](#) by Chris Peters
- [Understanding Server Applications](#) by Tom Jelen and Russ King
- [Your Nonprofit's Backup Strategy](#) by ONE/Northwest, Kevin Lo, and Elliot Harmon

Appendix

TechSoup IT Baseline Standards Goals, Objectives and Process for DV Agencies

The vision of *TechSoup IT Technology Baseline Standards* is to offer a set of targeted guidelines and recommended technologies that, when taken together, could provide a necessary foundation for building a healthy and secure Information Technology (IT) system. Our assumption is that by adopting or implementing these standards, domestic violence (DV) agencies will be better able to:

- Plan for and implement transformative technologies
- Integrate IT with programmatic functions
- Lower basic IT support costs
- Improve reliability of IT systems



Baseline Goals

Assist DV agencies to:

- Reduce instances of catastrophic computing failures
- Decrease the time and expense needed to support basic computing infrastructure
- Enable technology assistance providers to implement solutions according to sound tech principles at a minimal cost
- Be prepared for growth in your organization and its mission with a scalable IT infrastructure



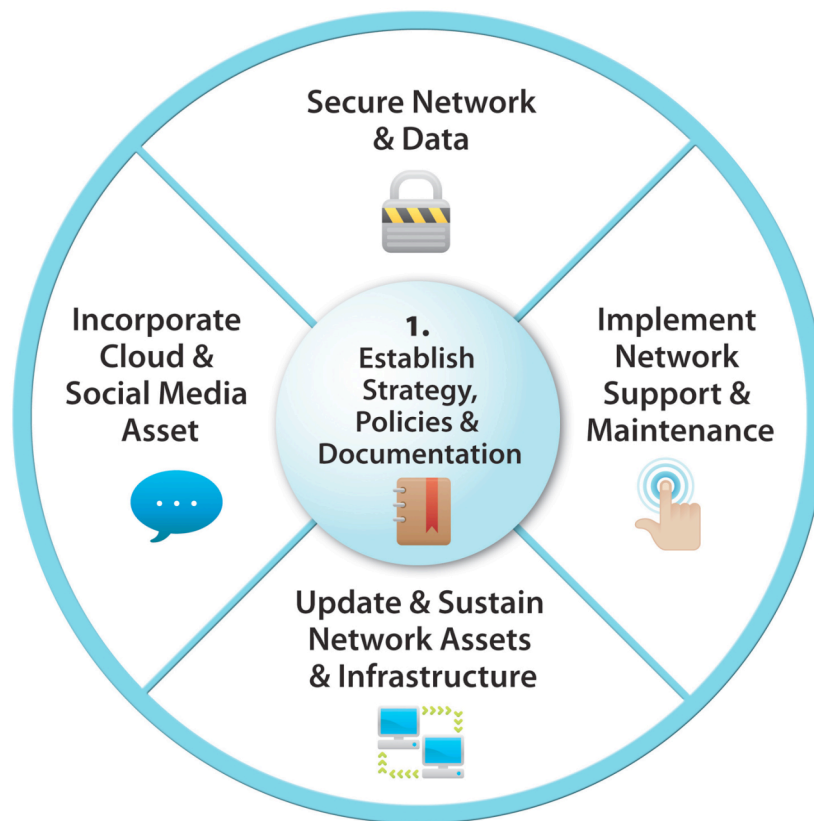
Baseline Objectives

Our initial objectives for the first year of the project are to:

- Increase organizations' ability to engage in smart IT planning and management
- Have all essential documentation completed
- Have an overall budget and fund development strategy
- Essential practices that will keep existing IT resources (network and data) secure

TechSoup IT Baseline Standards

The following are the baseline standards for creating a healthy and secure computing environment. The Baseline Process has been broken into 5 areas with essential tasks to be completed at each stage. These standards are not *necessarily* sequential and depending on an organization's "readiness", they may be able to complete some or all of these in this project year. However your organization should **always start with Establishing Strategy, Policies and Documentation** and then determine the appropriate next step.



TechSoup will work with and support DV agencies throughout this process and provide essential guidance and resources needed to achieve these standards through our webinar series, TechTalks, Forums, and feedback to DV agencies.



1. Establish Strategy, Policies, and Documentation

This first task will provide the essential foundation for all other activities. For this reason, we strongly recommend that all DV organizations complete this task before moving forward with other standards. This documentation will provide you with essential information regarding your computing assets and resources, as well as help you identify how technology serves and supports your organizational mission.

- **Technology Strategy:** A summary document outlining organizational strategic goals and how technology can support those goals. It will also have clear objectives for meeting those goals, including staffing assignments and a timeline.
- **Technology Resource Documentation:** An inventory of technology assets, policies, job descriptions, user login, and resources.
- **Technology Budget and Funding Strategy:** A budget that includes the costs and funding for hardware, software, hosted services, support contracts, training, and staffing (internal and/or external consultants).



Secure Network and Data

Security is a top priority when it comes to your organizational data and resources. For that reason, we strongly recommend that all DV organizations complete this stage as soon as possible after completing Stage 1. This stage will help you identify how you are currently keeping your information secure and how to protect it on a regular basis.

- **Define Network Support and Maintenance Systems:** Documentation of support and maintenance processes, including job descriptions, staff assignments and communication/reporting systems.
- **Data Privacy and Protection Process and Systems:** Documentation of data privacy policies, how data will be managed and stored, along with an encryption process that matches the organization's requirements.
- **Data Backup:** Documentation and scheduled data backup process and procedures are instituted on a regular basis.



Implement Network Support and Maintenance

After completing Standard 2 your organization will have a clear picture of what you need to secure and what your top priorities are. During this stage you will begin to implement some of those support and maintenance tasks and activities.

As a result, your organization will have a better-protected and operational computing system, as well as a more efficient staff and better-served clientele.

- **Secure Network Assets:** Install and manage network firewall, antivirus and anti-spam best practices, remove old user accounts, update current user passwords, and establish a physical security system that protects computer and network assets.
- **Implement Scheduled Support:** Implement regular network systems support checks, backup and virus protection checks, and provide regular user support opportunities.



Update and Sustain Network Assets and Infrastructure

Now that your organizational systems are more secure and efficient and your computing resources are being supported and maintained, it is time to update your computing systems and infrastructure. If you have completed the tasks and documentation identified in Standards 1-3, you now have a clearer picture of what essential hardware and software should be purchased and/or donated to your organization. During this stage, you will also tackle the "what if" of a disaster and develop a plan to protect your organization and its assets in the event of an emergency.

As a result, your network will be current with industry standards, and you'll have a plan to protect that investment if a disaster strikes.

- **Update Network:** Based on documentation and strategy, update hardware, software, and infrastructure assets in order of priority.
- **Establish a Disaster Plan:** Identify what the plan elements include and assemble necessary tools and resources to make it happen.
- **Revise Budget:** Revise line items for long-term support needs, including schedule support, user support, technology projects, and system obsolescence.



Incorporate Cloud and Social Media Asset

During this phase of development we encourage you to explore some of the newer technologies, resources, and options available to organization through "cloud computing". We also advocate that you explore social media options and assess its value towards enhancing and supporting your mission.

- **Explore Cloud Providers Alternative:** Depending on the needs and requirements of the organization, identify cloud providers that can complement or replace existing IT infrastructure and processes.
- **Explore Social Media Adoption:** Explore social media adoption based on safe computing habits and standard social media policies.
- **Collect and Report on Organization-Wide Data:** Collect and report data by reviewing dashboards, analytics, and standardized metrics.

Information Technology (IT) Manager

This is the critical but often overlooked role. To successfully build and manage your information and technology (IT) systems, you need a person with a deep understanding of your organization's strategic goals and mission. That person will also need to have a vision and understanding of how IT can strengthen and support your mission and organization.

It is highly recommended that the ISP be a member of your organization's Management Group. That way IT and Information Systems are at the same level as other essential systems and departments in your organization including but not limited to Human Resources, Finance and Fund Development.

We strongly suggest that you identify a staff person to serve as your ISP, because operating without a management-level staff person responsible for the Information System Planner's tasks is not IT management by design - it is IT management by luck.

What Makes A Good Information Technology (IT) Manager?

The ideal candidate should be able to demonstrate the following:

- A thorough understanding of the organization's culture and the ways in which technology is used to further the mission of the organization
- A strong interest in, and understanding of, technology issues and resources
- A "people person" with strong Interpersonal skills and an ability to serve as both a team member and a team leader
- Strong project manager who brings an ability to handle multiple projects of various sizes and complexity at the same time
- Can solve problems related to IT and assign appropriate resources
- Experience writing and/or reviewing budgets with a capacity to estimate project costs and schedules with a degree of accuracy
- Effectively facilitate meetings with internal and external staff
- Analyze and define problems and solutions
- Communicate effectively both verbally and in writing
- Knowledge of technology administration and systems or has team of subject matter experts (SME) to inform and guide decisions
- A good understanding of technology, be able to develop strategies, oversee implementation and manage staff

[continued]



What Does An Information Technology Manager Do?

The IT Manager works closely with any IT support personnel, as well as information system planning staff. Their role includes overseeing and supervising all work completed by the network/computer support staff (and vendors), as well as insuring that essential IT tasks and activities are completed (i.e. back-ups, network security updates, etc). They are responsible for forwarding IT support and infrastructure questions and requests to appropriate channels, so they can make key decisions regarding inventory purchases and infrastructure needs. The IT Manager also provides recommendations to managers, directors and board members regarding future IT strategies and resources that will support the organization's mission.

JOB PROFILE: INFORMATION TECHNOLOGY MANAGER

Examples of Some Information Technology (IT) Manager Tasks

- Manages relationship with vendors, contractors, and service providers
- Creates and updates technology plans, policies, and strategies
- Budget for and approve technology funding in the organization
- Designs, maintains, and reviews organization-wide IT policy
- Be a core member of the technology team
- Makes final decisions for hardware and software standards
- Supervise and mentor staff
- The IT Manager must be able to do the necessary research and ask the necessary questions regarding IT projects. The research and questions must concern available options, product support, cost in direct dollars, cost in maintenance, cost in staff resources, and training requirements.



What Training Does An IT Manager Need?

As with the Accidental Techie, the IT Manager can gather their initial technical training by completing a certification or academic program, as well as from “on the job” training. Depending on the organization, your training may be enough to enter the job. However, technology is one of the fastest moving and changing industries and so it will be critical to build in time to grow and update your skills and knowledge on an ongoing basis. For the IT manager you will also have the added training requirements in the areas of project management as well as analysis and forecasting.

Accidental Techie

The Accidental Techie is the “go to” person for keeping an agency’s computers and computer network (if you have one) up and running. They are the first person contacted when an organization needs to identify and deal with Information Technology (IT) problems, as well as providing basic staff and user support.

At times the Accidental Techie could be asked to help make decisions about the direction and future IT systems for your organization. While it might be the Executive Director or in some cases the Controller or Operations Officer’s job to make decisions about managing and building your computer and IT systems, the Accidental Techie may well be the person responsible for implementing the agency’s technology plans and policies, and keeping systems operational.

What Makes A Good Accidental Techie or IT Person?

You could be an Accidental Techie if you:

- Like people
- Like technology
- Interest in sharing technical information with others
- Enjoy “fixing” things
- Not afraid to break things
- Like to learn new things
- Able and willing to take chances
- Ability to do multiple tasks at the same time
- Willingness to look at and read/review manuals
- Interest in exploring new information that leads to solutions (both in manuals and online)
- Good sense of humor (don’t take yourself or technology too seriously)
- Ability to solve problems (start with the obvious answer and then graduate to more complex solutions)
- Ability to explain problems and solutions in a variety of ways: visual, audio, hands-on, 1-1, classroom, tutoring, etc.

Examples of Some Accidental Techies Tasks

- Set up new computers
- Move computer data from one workstation to another
- Install new hardware and software for one or many (networked) computers
- Customize computers to fit the needs of your organization (add memory, configure hard drives, connect internal and external printers, etc.)



What Does An Accidental Techie Do?

An Accidental Techie, works closely with Executive staff and responds to user problems as required. If the organization has a computer network they will most likely serve as the manager or “systems administrator” for some or all of the hardware (computers, phones, printers) or software (database, e-mail) problems. Although many of the specific tasks of system maintenance may fall to others within the organization, or to an outside vendor, the Accidental Techie will probably be the first person contacted if there is a computer problem.

[continued]

JOB PROFILE: ACCIDENTAL TECHIE

Examples of Some Accidental Techies Tasks [continued]

- Track and update IT inventory and documentation for hardware and software
- Make sure all of the computer backups are working and key data is being captured
- Oversee or do computer infrastructure and wiring upgrades
- Troubleshoot Windows or Mac OS problems
- Troubleshoot individual or computer networks within your organization
- Update and manage all software updates and virus/malware definitions
- Write and maintain documentation (i.e. all hardware and software serial numbers, vendor contacts, location of IT resources, etc.) in a central location
- Attend regular meetings with Executive Director or the manager of your IT systems to maintain good systems and IT practices

The Accidental Techie Could Be Expected To:

- Consult with managers regarding IT plans and policies
- Solve user problems, system problems, and network errors independently
- Work with Executive Director (or other senior manager) to prepare budget or other reports as required
- Work with vendors, contractors, and service providers to coordinate additional technical services
- Conduct and lead trainings and tutor staff
- Accidental Techie resources to review and explore
- Compass Point's Accidental Techie Book
- Accidental Toolkit from TSG Learning Center (To Be Developed)



What Training Does An Accidental Techie Need?

Accidental Techie can have formal training or “on the job” experience depending on the organization’s needs. IT training may be enough to enter the job, however, technology is one of the fastest moving and changing industries and so it will be critical that this person build in time to grow and update their skills and knowledge on an ongoing basis.

If you or someone you know is interested in becoming an Accidental Techie, we suggest you share this job description with your immediate supervisor and/or the person responsible for the organization’s technology systems. Once you’ve identified the right person for the job, be sure there is a plan for reviewing their existing IT skills and then schedule time for them to acquire and utilize new skills.

Information Systems Director

The ISP is responsible, at the highest level, for budgeting, approving, funding, and working with the IT staff to create technology plans, policies, and strategies.

One person with strategic knowledge of the organization's mission and culture is needed to think about the role of IS (Information Systems) in achieving that specific mission within that specific culture. This position is the critical role. Whatever other IS/IT roles or positions taken on within your organization, the ISP role must be accounted for in order to have a successful Information Technology system.

It is also important that the ISP be at the same organizational level as any member of the Management Group. Without the structured support of this role, it is impossible to implement any long-term IT planning or projects successfully. Even short-term projects may be doomed because of conflicting, contradictory or unclear goals. Operating without a management-level staff person responsible for the Information System Planner's tasks is not management by design - it is management by luck.

What Makes A Good Information Systems Director?

The ideal candidate should be able to demonstrate the following:

- Ability and willingness to act as an appropriate technology advocate
- Ability to make management-level financial decisions about expenditures and fundraising
- Management experience to oversee all IT staff and consultants, and other technology resources
- Ability to work on a team
- Strong interest in technology
- Ability to analyze cost/benefit information and make decisions appropriately
- Understanding of the strategic plan of organization
- Understanding of the organization's mission
- Understanding of budget process
- Meeting facilitation skills
- Excellent communication skills, written and oral

Example of Some Information Systems Director Tasks?

- Budgeting, approving, funding and creating technology plans, policies, and strategies
- Designs, maintains, and reviews IS policy
- Member of technology team
- Makes final decisions for hardware and software standards
- Approves all IS projects
- IS advocate to other executives and board
- Ensures IS operates in-step with strategic plan
- Ensures IS operates in-step with organization's mission



What Does An Information Systems Director Do?

An Information Systems Director oversees all IT staff. While the IT manager makes technology recommendations (upgrades, software installation, documenting networks, etc.), it is the ISP who makes the final decisions on the plans, policies, and strategies.



What Training Or Background Does An Information Systems Director Need?

The ISP should have a broad understanding of technology and be able to develop strategies, oversee implementation, and manage staff. The ISP also needs financial planning experience to budget and make expenditure decisions.

The ISP should have a thorough understanding of the organization's culture and the ways in which technology is used to further the mission of the organization.

The ISP does not need to be a programmer or network administrator. However, he or she should have a general knowledge and interest in technology issues, with good research and analysis skills

BSAV Product Offerings

BSAV grantees can request anything within the TechSoup catalog as long as your organization is eligible according to each donor partner's guidelines. However, we suggest that grantees first review the recommended products below. These address many of the identified needs and issues gathered through a survey of Blue Shield grantees. Again, this is a suggested list and does not preclude organizations from requesting other products or services, rather it is meant to serve as a starting point for organizations that are unclear about what is available and what might be most appropriate for their organizations.

→ BSAV Recommended Hardware

TechSoup's [Refurbished Windows Computers](#) are broken down into tiers (high, mid, and low). Mid-tier computers are sufficient for most standard office tasks. High-tier computers are appropriate if you will be using the computer for more resource-intensive tasks such as web publishing and editing images or video.

- [Refurbished Desktop/Monitor Bundles](#)
- [Refurbished Mid-Tier Desktop Computers](#)
- [Refurbished Mid-Tier Notebook Computers](#)

[Six 1-hour Flip MinoHD video cameras](#): This bundle includes six Flip MinoHD 4 GB video cameras. These cameras are very easy to use and are great tools for digital storytelling.

→ BSAV Software Favorites

Security Resources

- For very small organizations with only a few computers: [Symantec Norton Antivirus 2012](#) (antivirus/anti-spyware) or [Symantec Norton 360](#) (also includes data backup).
- For larger organizations that want to centralize security management: [Symantec Endpoint Protection](#) includes antivirus/spyware, firewall, and other security features. This product is most suitable for organizations with between 5 and 100 computers.

Office Productivity

- [Windows 7](#) operating system
- [Microsoft Office](#) (note: MS Office is included with some of TechSoup's refurbished computers, so if you are also requesting a computer, you may not need Office)
- [Microsoft Office for Mac](#)

Accounting

- [Intuit QuickBooks 2011](#): manage essential financial tasks like paying bills, creating invoices, producing reports, and tracking expenses, contributions, and payments.

Suitable for small to medium-sized organizations.

- [AccountEdge](#): financial management software for small or medium-sized organizations. In addition to basic features like banking, sales and expense tracking, and customer management, AccountEdge also helps organizations manage purchases and payables, inventory, and payroll.
- [Sage Peachtree Accounting for Nonprofits](#): provides accounting and analysis tools to help nonprofit organizations improve their financial management. It is suitable for organizations with 50 or fewer employees.

Audio and Web Conferencing

- [ReadyTalk](#) audio and web conferencing one-year subscription: meet and collaborate on the phone and on the web. This product includes discounted audio conferencing, free web conferencing for up to 25 participants, and other discounted services.
- [BetterWorld](#) audio conferencing: discounted pricing for BetterWorld's audio conferencing services that allow organizations to collaborate on the phone using their existing phone systems.
- [GoToMeeting](#) one-year subscription: online web conferencing tool that allows up to 15 users and a host to meet and collaborate on the web and on the phone.

Fundraising, Donors, Contact Relationship Management (CRM)

- [BlackbaudNow](#): BlackbaudNow is free online software that provides small organizations with the tools to create a donation-ready website, powered by PayPal, as well as manage donors and run email marketing campaigns. The TechSoup donation adds access to MatchFinder, which allows organizations to search Blackbaud's database of more than 24,000 companies in North America that match gifts from employees.
- [DonorPerfect](#): a web-based tool for fundraising and donor management. This donation provides for databases of up to 1,000 records.
- [eTapestry](#): web-based software for fundraising and contact management for donors and other contacts. This donation is most appropriate for organizations with 500 to 1,000 records.
- [GiftWorks Standard](#): fundraising and donor management software designed for nonprofits. Organizations can use it to track donors and donations, create standard and customizable reports, send mailings, and build targeted lists of donors, supporters, and prospects.
- [Sage ACT! Pro](#): a contact management and productivity application for individuals and small groups. It can be used to track the history of interactions with each contact or organization and the overall status of a campaign. It also contains e-mail templates and scheduling features that help organizations create multi-step marketing campaigns and maintain regular communication with actual and potential supporters.

Data Collection and Analysis Tools

- [FluidSurveys](#): a web-based tool for creating online surveys and collecting and analyzing survey data. No programming or design experience required.
- [FileMaker Pro](#) database software.
- [Microsoft Access 2010 database software](#) (Note: MS Access is included in Pro versions of Office).

Creating Images, Video and Audio

- [Adobe application suites for Windows](#)
- [Adobe individual software products for Windows](#)

Training

- [easyLearning](#) offers over 1,500 online courses on technology topics ranging from computer basics to Microsoft Office to sophisticated software development and programming. They also offer professional and business skills courses.
- [QuickBooks Made Easy for Non-Profits live seminar](#)
- [QuickBooks Made Easy for Non-Profits training CD-ROM](#)

Servers and Networking

- Server software: [Microsoft Small Business Server](#) provides small organizations with many of the features used by large organizations — file and printer sharing, an email server, tools to manage Internet access, internal websites (intranets), remote access, support for mobile devices, and backup/restore tools — in an integrated product.
- We also offer a wide variety of [Cisco products](#) for setting up and securing your organization's network.

How to Request Your Donation With TechSoup



Before You Request Your Donation

- Register your organization at www.TechSoup.org
- Review your technology resources and request products based on your organization's needs:
 - Identify the products that best fit your needs
 - Make sure you are eligible to request that donation
 - The total cost does not exceed \$1250



How to Request Your Donation

- Log into your account at TechSoup
- Add products to your cart to total **\$1250. Remember you have one chance to purchase your products.**
- Click on **Check out**
- Choose **ground shipping**
- For the payment method choose the “**check**” option which accesses your donation allotment
- You will receive a TechSoup order confirmation email



After Requesting Your Donation

Watch the Technology Capacity Project webinars including:

- [Webinar #1 – Introduction to BSCF Technology Capacity Project](#)
- [Webinar #2 – Technology Planning](#)
- [Webinar #3- Security](#)



To Complete Your Order

You **must** forward the confirmation email to BSCFgrant@techsoup.org to complete the donation process.



Donation distributions will begin 10 working days after you request your donation.

Need Help? Contact Ricci Powers at ricci@techsoupglobal.com

Technology Capacity Building: E-Learning Series

The Technology Capacity webinar series is available to BSAV grantees who are interested in learning more about this project, as well as how to better manage your computer and information systems. You can view each webinars any time that is convenient for you, simply by going to the YouTube links listed below. You can also download the PDF of each webinar if you would like to review the presentation at a later date.

The first webinar will provide you with an introduction to the project along with key resources. The second and third webinars will focus on key elements for building your technology capacity.

Once you have watched each webinar we suggest you check the “Review and Questions”. These pages will highlight key concepts from each webinar, as well as point you to helpful resources discussed during each session.



Webinar # 1

[Getting the Most from TechSoup and the Technology Capacity Project](#)

A webinar highlighting what is available through TechSoup and the Technology Capacity Project

[Webinar #1 PDF](#)



Webinar # 2

[Information and Computing Systems Policies and Documentation](#)

During this webinar we will share with you how to gather and organize your technology resource information before moving forward with making decision regarding what to buy and how much to spend.

[Webinar #2 PDF](#)



Webinar #3

[An Introduction to Security Basics/Fundamentals](#)

Security is a top priority when it comes to your organizational data and resources. For that reason, we strongly recommend that all DV organizations complete this stage as soon as possible after completing Stage 1. This webinar will help you identify how you are currently keeping your information secure and how to protect it on a regular basis

[Webinar #3 PDF](#)



Technology Capacity Project Guides

The Technology Capacity Project Guides serves as resource and complements to the webinar series. The guides are designed to provide the DV community with the tools and information you need to manage your IT systems effectively. Throughout the webinars you will hear references to tips, tools and resources contained in the guide. For that reason we strongly suggest you download the project guides before viewing the webinars.

- *An Introduction to the Technology Capacity Project*
- *The Technology Capacity Project Guide – How to Manage Your IT Systems*
- *An Introduction to the TechSoup Forums*

Webinar #1 Review Questions

Slide numbers refer to the slide in the PowerPoint presentation entitled "Introduction to BSCF Technology Capacity Project". Page number's refer to pages (as number at the bottom left of the page) in the PDF guide entitled "Technology Capacity Project Guide".

1. Based on TechSoup's survey what are the 3 top challenges facing DV organizations?
Slide 11
2. What 4 services are being provided by TechSoup to Grantees to address those challenges?
Slide 12
Intro to the TCP Guide page 2
3. What is the total amount of donated product that grantees can receive if they complete the grant requirements?
Slide 13
Intro to the TCP Guide page 3
4. What are two training resources that you will be able to receive through this project?
Slide 15
Intro to the TCP Guide pages 4-6
5. A grantee must complete how many webinars to be eligible to request free products through TechSoup?
Slide 19
Intro to the TCP Guide page 3
6. What is the 5-step process for Getting Started with your Product Donations
Slide 26
How-To-Request-Donations Instruction sheet
7. Where can you go to find the product that your organization is eligible to receive?
Slide 34
TCP Guide page 31
8. What are the goals of the capacity building project?
Slide 10
TCP Guide pages 56
9. What is the value online peer support?
Slide 16
How to Use TechSoup Forums Guide
10. Is assistance available through TechSoup to register your program and select the right products for your organization? Y__ N__
Slide 14
TCP Guide page 12

Webinar #2 Review Questions

Slide numbers refer to the slide in the PowerPoint presentation entitled "Technology Planning". Page numbers refer to pages (as number at the bottom left of the page) in the PDF guide entitled "Technology Capacity Project Guide".

1. What are the 5 steps to developing a technology strategy?
Slide 9
The TCP Guide page 5
2. Where can I find an inventory worksheet in my technology capacity planning guide?
The TCP Guide Toolkit pages 4-11
3. What minimum items should we include in our technology budget and where can I find a worksheet to help with this?
TCP Guide page 14
4. What are the 5 baseline standards for a healthy and secure computing environment?
TCP Guide page 18 or TCP Toolkit pages 1-5
5. What are four Policy documents that you'll want your organization to have?
The TCP Guide page 11
6. Who should you contact at TechSoup if you want assistance or have questions?
Slide 53
7. What are the 3 P's of Implementation?
Slide 40
8. Why do you need a technology strategy?
Slide 10-16
TCP Guide page 4
9. When making decisions about technology purchases consider not only "What do we want to buy?" Think about "What do we want to ___?"
Slide 29
10. What resource in the TCP Guide will help you identify what IT resources your organization has and needs?
Slide 43
TCP Guide Section 3
11. Who will complete the inventory worksheet for your organization?
The TCP Guide Toolkit pages 4-11

Webinar #2 Review Questions

Slide numbers refer to the slide in the PowerPoint presentation entitled “Healthy and Secure Computing for Domestic Violence Agencies”. Page number’s refer to pages (as number at the bottom left of the page) in the PDF guide entitled “Technology Capacity Project Guide”.

1. Provide one key reason why data privacy and security matters for Domestic Violence Agencies?

Possible Answers (Slide 13 & Page 39)

- DV organizations’ constituents especially concerned with privacy
- Stealing and selling personal information is big business
- Information security breaches can result in major legal problems

2. What is the top threat to data security?

Possible Answers (Slide 12 & Page 40)

- Viruses, spyware and other malware

3. What kinds of data are considered sensitive for most organizations?

Possible Answers (Slide 19 - discussed not written & Page 41)

- Name, address, phone numbers
- E-mail addresses Social Security number
- Credit card and banking/financial information
- Health and medical records

4. What do data retention policies refer to?

Possible Answers (Slide 19 - discussed not written & Page 42)

- Rules for what data must be kept, and how data is disposed of
- Identifies what data should be destroyed, and procedures for doing this

5. What technologies can be used to help keep data secure?

Possible Answers (Pages 42/44 and Slides 26/27)

- Locked rooms for computers, servers and storage devices
- Firewalls
- Antivirus / anti-spyware
- Data encryption

6. Why should we be extra cautious about data security on mobile devices?

Possible Answers (Page 44, Slides 12, 27 - discussed not written)

- Easy to lose these devices
- Easy for these devices to be stolen

7. What are minimum basic technology safeguards organizations should plan to implement?

Possible Answers (Page 44, Slide 22)

- Backup system
- Virus protection
- Password policy
- Firewall
- Data encryption

8. How should access to sensitive data be controlled?

Possible Answers (Page 44, Slide 25)

- Both physically and electronically

9. What are some key principles to strong passwords?

Possible Answers (Pages 47, 48, Slide 26 - discussed not written)

- Long
- Complex
- Hard to guess
- Changed frequently
- Vary between accounts

10. Why is having a private conversation on social media tools a bad idea?

Possible Answers (Page 52, Slide 31)

- Social media is based on personal exposure
- Social media core business model is to learn and share who you are with others
- Social media companies frequently change their privacy settings, exposing private information

11. What is the benefit of password protected screen savers?

Possible Answers (Page 51, Slide 27)

- They automatically lock a computer when left unattended
- They force a login and password to gain access to an unattended computer

12. What steps should your organization take if you suspect a security breach?

Possible Answers (Page, 51, Slide 28)

- Report the breach immediately to the designated person
- Change passwords to compromised systems
- Follow legal obligations and ethical/policy guidelines for reporting breaches to your constituents

13. What are some ways to inform your constituents about how to access your services safely?

Possible Answers (Pages 51-52, Slide 7)

- Notify constituents of your privacy policy
- Post the privacy policy on your website
- Explain how to browse the web safely (clear browser history/cache, search history)
- Offer multiple methods to contact you
- Explain to constituents how to protect their email
- Refresh staff on policies regularly
- Show secure data exchange



How to Use TechSoup Global Forums

Strengthening your
technology systems
to better serve
your community

Contents

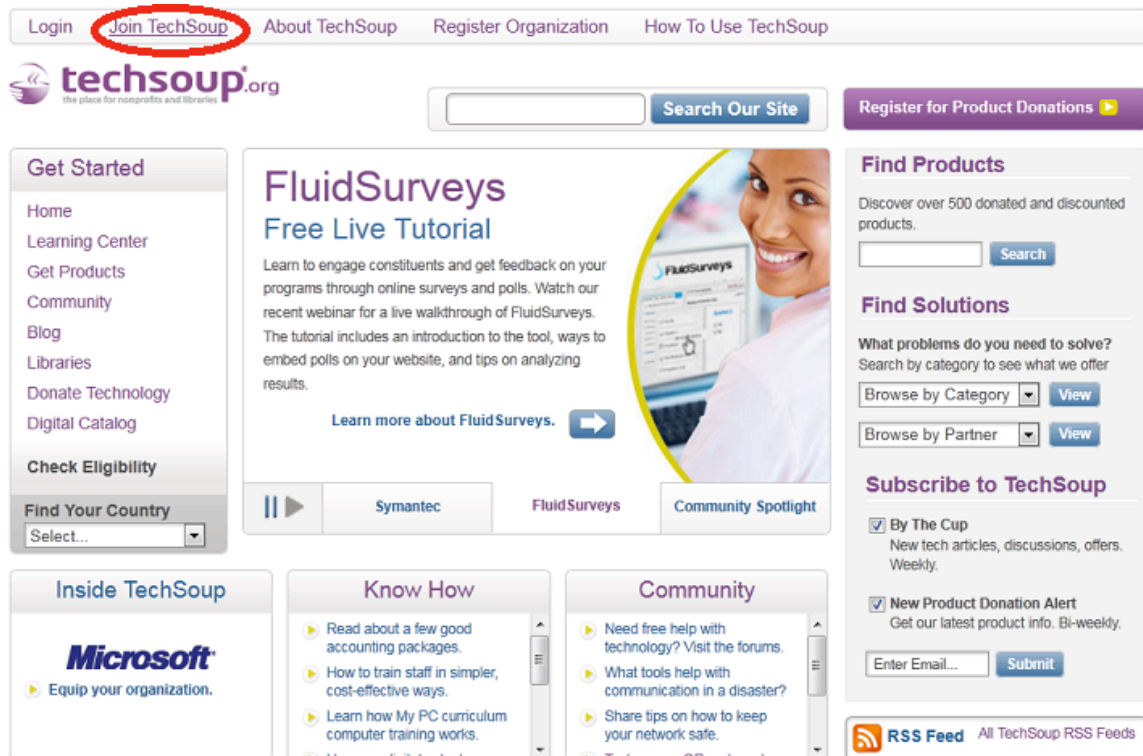
- How to Register for TechSoup Forums 1
 - Join TechSoup 1
 - Create a Member Profile 2
- Getting Started on TechSoup Forums 5
 - Introduce Forum..... 5
- How to Participate in TechSoup Forums..... 7
 - Categories 7
 - Search Community 8
 - How to Ask a Question..... 8
 - Question Samples..... 9
- How to Get Technical Help 11

How to Register for TechSoup Forums

→ Join TechSoup

To participate in the TechSoup forums, begin by setting up your user profile.

1. Go to www.techsoup.org
2. Click on **Join TechSoup** in the upper left-hand corner



3. An “Enter Your Information” screen will come up. Fill out your member information and create a Member Name.

Your member name is displayed to other users when you participate in TechSoup community forums, and is not used to log in. Your member name can't be changed, so create a member name you'll want to keep.

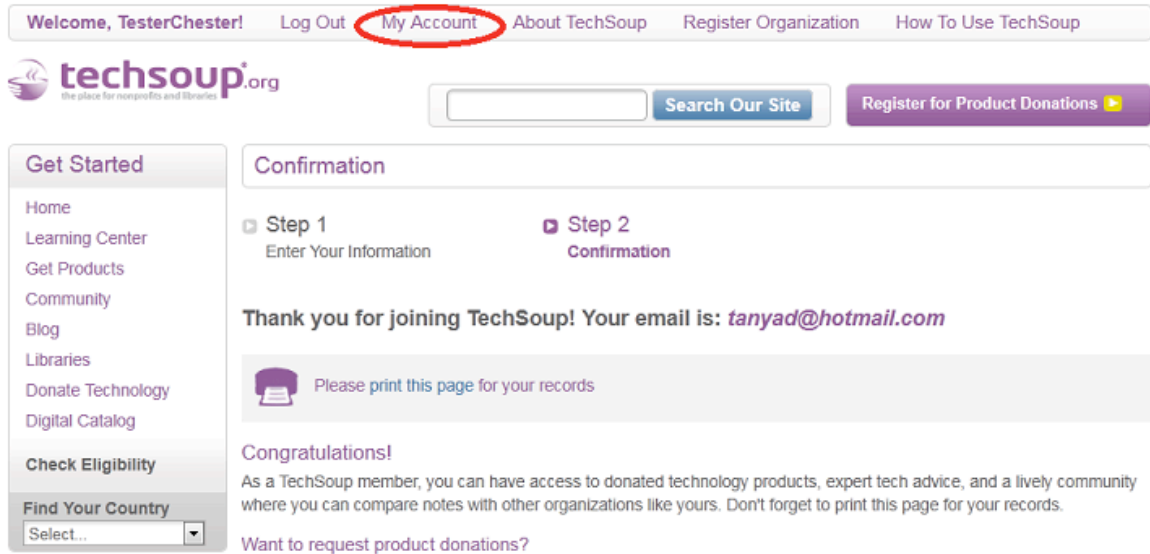
Anonymity and pseudonymity are permitted in the TechSoup community, but think about making your Member Name clear and straightforward.

Create a security question you will remember the answer to. If you lose your password, this will come in handy.

4. Complete the information and click the **Join TechSoup** button at the bottom of the page. (Keep up with TechSoup's news and products by subscribing to the newsletters.)

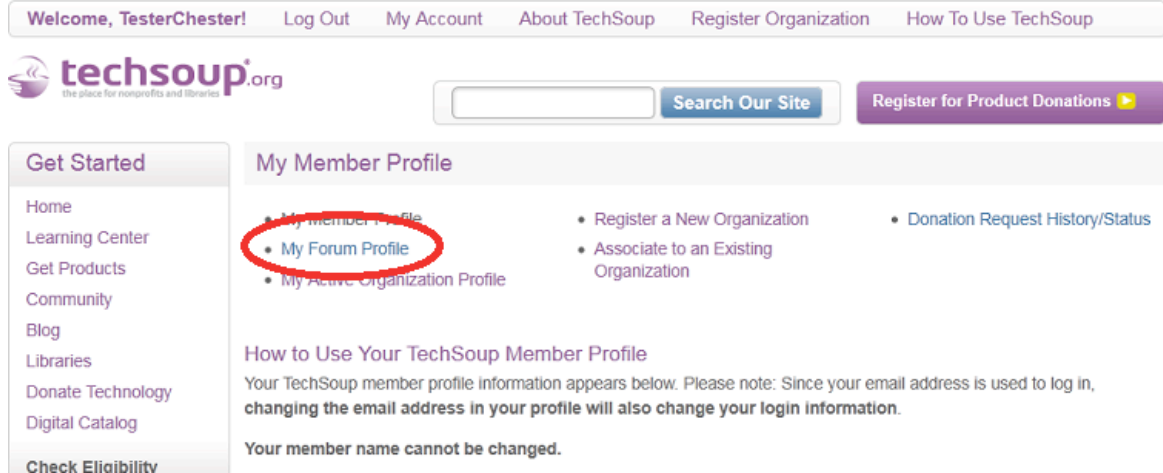
→ Create a Member Profile

1. From the confirmation screen, click on the **My Account** link at the top of the page, which will take you to the My Member Profile page.



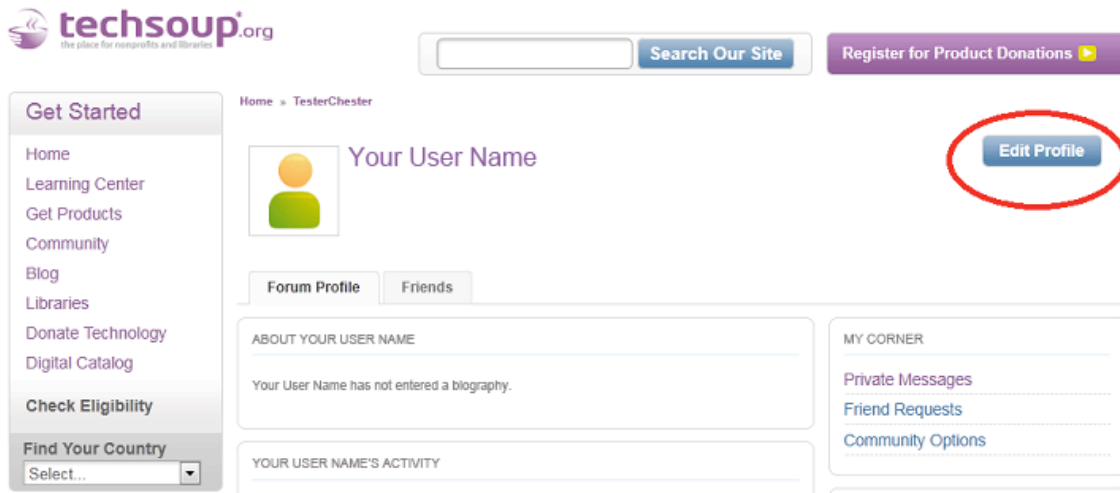
The screenshot shows the TechSoup website's confirmation page. At the top, a navigation bar includes links for 'Welcome, TesterChester!', 'Log Out', 'My Account' (circled in red), 'About TechSoup', 'Register Organization', and 'How To Use TechSoup'. Below the navigation bar is the TechSoup logo and a search bar. A sidebar on the left contains a 'Get Started' menu with links to Home, Learning Center, Get Products, Community, Blog, Libraries, Donate Technology, and Digital Catalog. The main content area is titled 'Confirmation' and shows two steps: 'Step 1: Enter Your Information' and 'Step 2: Confirmation' (the active step). A message reads: 'Thank you for joining TechSoup! Your email is: tanyad@hotmail.com'. Below this is a printer icon and the text 'Please print this page for your records'. A 'Congratulations!' message follows, stating that as a member, users can access donated technology products, expert tech advice, and a community. At the bottom, there is a question: 'Want to request product donations?'.

2. Click on **My Forum Profile**



The screenshot shows the TechSoup website's 'My Member Profile' page. The navigation bar at the top is identical to the previous screenshot, with 'My Account' circled in red. The sidebar on the left is also identical. The main content area is titled 'My Member Profile' and features a list of links: 'My Member Profile', 'My Forum Profile' (circled in red), 'My Active Organization Profile', 'Register a New Organization', 'Associate to an Existing Organization', and 'Donation Request History/Status'. Below the links is a section titled 'How to Use Your TechSoup Member Profile' with the following text: 'Your TechSoup member profile information appears below. Please note: Since your email address is used to log in, changing the email address in your profile will also change your login information. Your member name cannot be changed.'

3. To edit your profile, click on **Edit Profile**

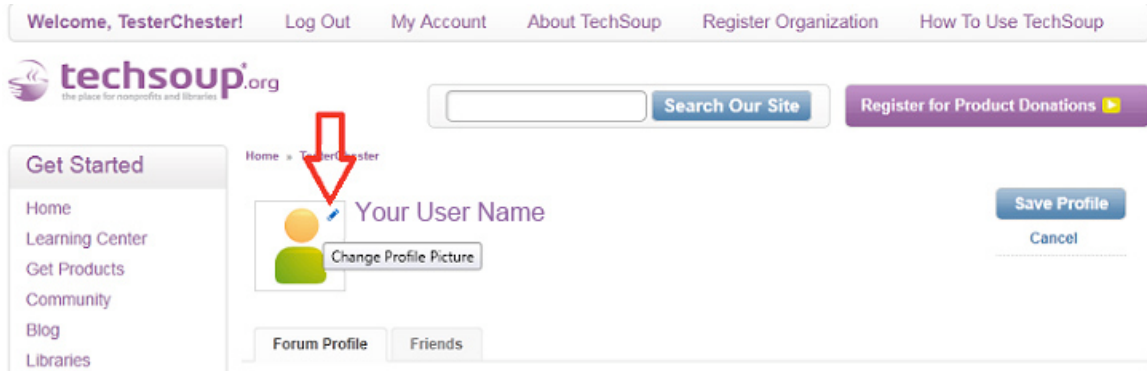


4. Fill out your profile as completely as possible, including a bio and picture. Again, anonymity and pseudonymity are permitted in this community, but complete profiles help build trust and credibility in the community. You may also add a public email if you want to be contacted.

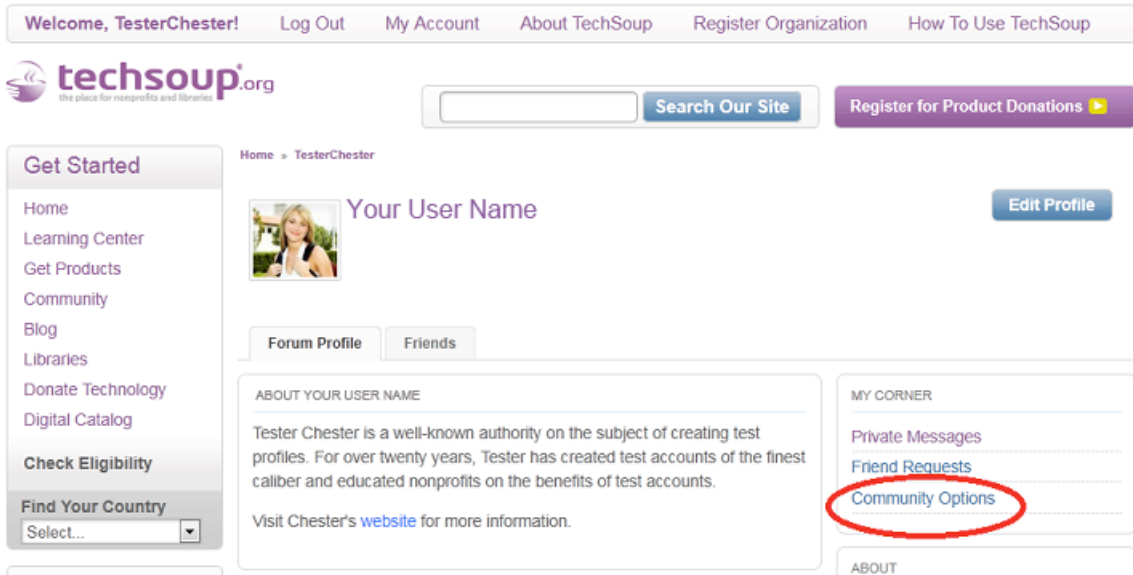
We understand that online safety is important and that when working with victims of domestic violence, anonymity is sometimes preferred. There are ways to remain anonymous and still complete a profile and have a picture. Your bio can be as simple as "I work at a nonprofit and am interested in connecting with others at nonprofits." Your picture may be of just about anything appropriate: if you are not comfortable using your own picture for any reason, a scene from nature, a pet, or something else is acceptable.

More information about filling out your TechSoup profile can be found [here](#).

- To upload an image, click the pencil icon on the profile image, and follow instructions to upload your photo. While an image is strongly encouraged, it does not have to be your own picture.



- Click on the **Save Profile** button and then click on **Community Options**.



- On the **Community Options** page you can toggle your personal display settings and create a signature line. Your signature line will further help identify you to the TechSoup community. Please include your job title and organization, and contact information if you would like to be contacted. This is not required, but can come in handy if your goal is to network with other nonprofits.

Now you're all set to participate in the TechSoup forums!

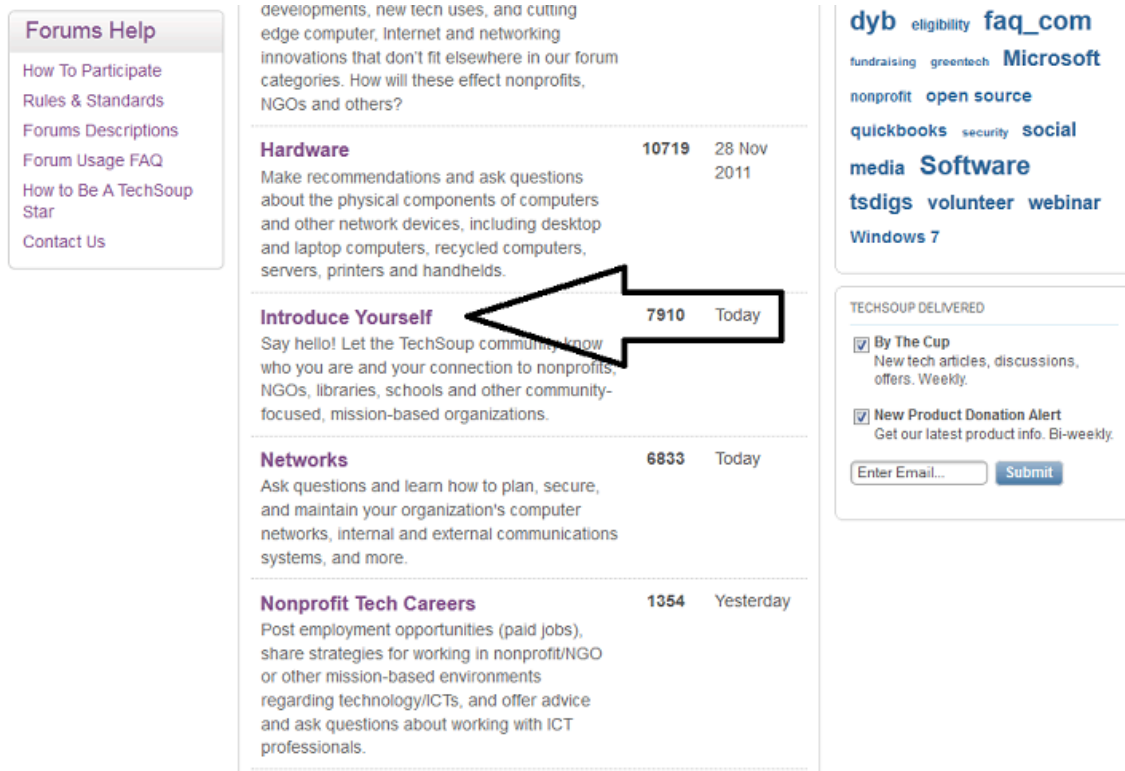
Getting Started on TechSoup Forums

Now that you've gotten your profile set up, it's time to explore what the TechSoup forums have to offer. With twenty categories to choose from, it can be a bit overwhelming (even for us!).

→ Introduce Forum

1. Click on this [link](#) and let's visit the TechSoup Forums.

Once you're there, a great place to start is in our **Introduce Yourself** forum. This is a friendly place to get yourself oriented and make your first post. Our longtime volunteer moderator Sasha Daucus, a communications professional with a fundraising software company that serves nonprofits, hosts this forum. Click on the **Introduce Yourself** title.

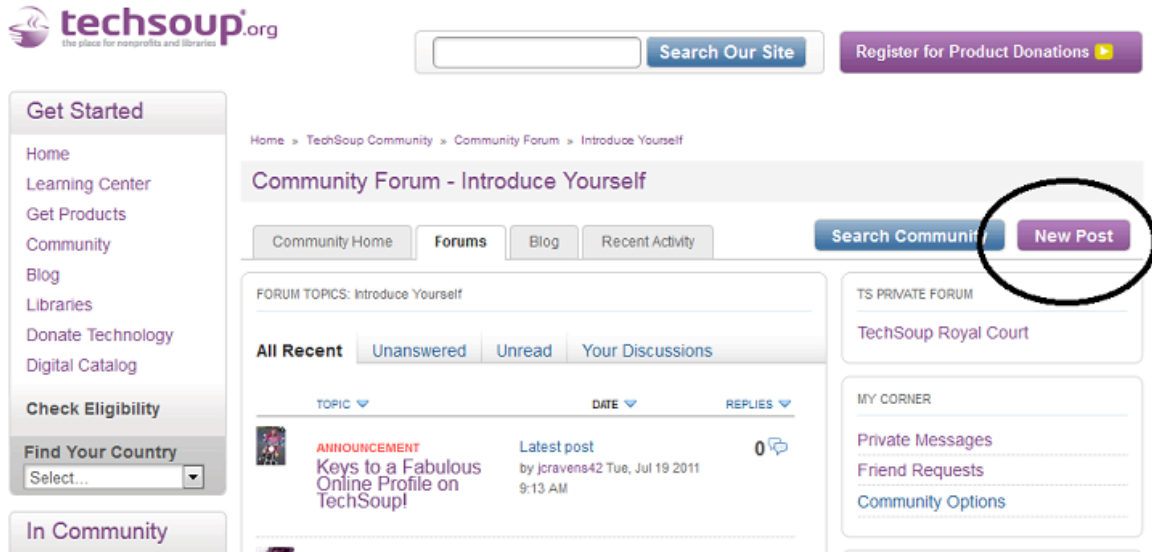


The screenshot shows the TechSoup Forums homepage. On the left is a 'Forums Help' sidebar with links like 'How To Participate', 'Rules & Standards', and 'Contact Us'. The main content area lists several forum categories with their respective post counts and dates:

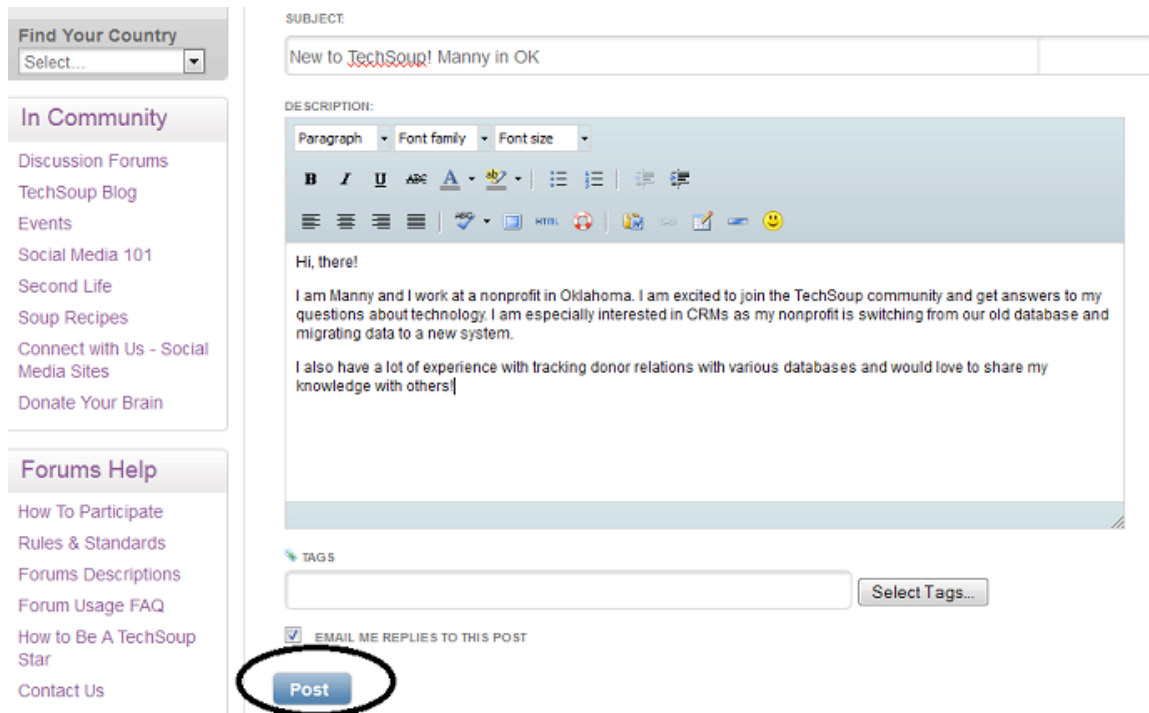
- Hardware**: 10719 posts, 28 Nov 2011. Description: Make recommendations and ask questions about the physical components of computers and other network devices, including desktop and laptop computers, recycled computers, servers, printers and handhelds.
- Introduce Yourself**: 7910 posts, Today. Description: Say hello! Let the TechSoup community know who you are and your connection to nonprofits, NGOs, libraries, schools and other community-focused, mission-based organizations. This category is highlighted with a large black arrow.
- Networks**: 6833 posts, Today. Description: Ask questions and learn how to plan, secure, and maintain your organization's computer networks, internal and external communications systems, and more.
- Nonprofit Tech Careers**: 1354 posts, Yesterday. Description: Post employment opportunities (paid jobs), share strategies for working in nonprofit/NGO or other mission-based environments regarding technology/ICTs, and offer advice and ask questions about working with ICT professionals.

On the right side, there are navigation links for various topics like 'dyb', 'eligibility', 'faq_com', 'fundraising', 'greentech', 'Microsoft', 'nonprofit', 'open source', 'quickbooks', 'security', 'social', 'media', 'Software', 'tsdigs', 'volunteer', 'webinar', and 'Windows 7'. Below that is a 'TECHSOUP DELIVERED' section with checkboxes for 'By The Cup' and 'New Product Donation Alert', along with an email input field and a 'Submit' button.

2. You can start with a post introducing yourself to the TechSoup community. Click on the **New Post** button on the right hand side of your screen.



3. Give your post an appropriate subject title and body (say hello and let us know who you are and why you're here). When you're done click the **Post** button in the lower left hand of your screen.



You've now made your first post on TechSoup and are ready to dive into our various topics to ask questions, network, and share knowledge.

How to Participate in TechSoup Forums

→ Categories

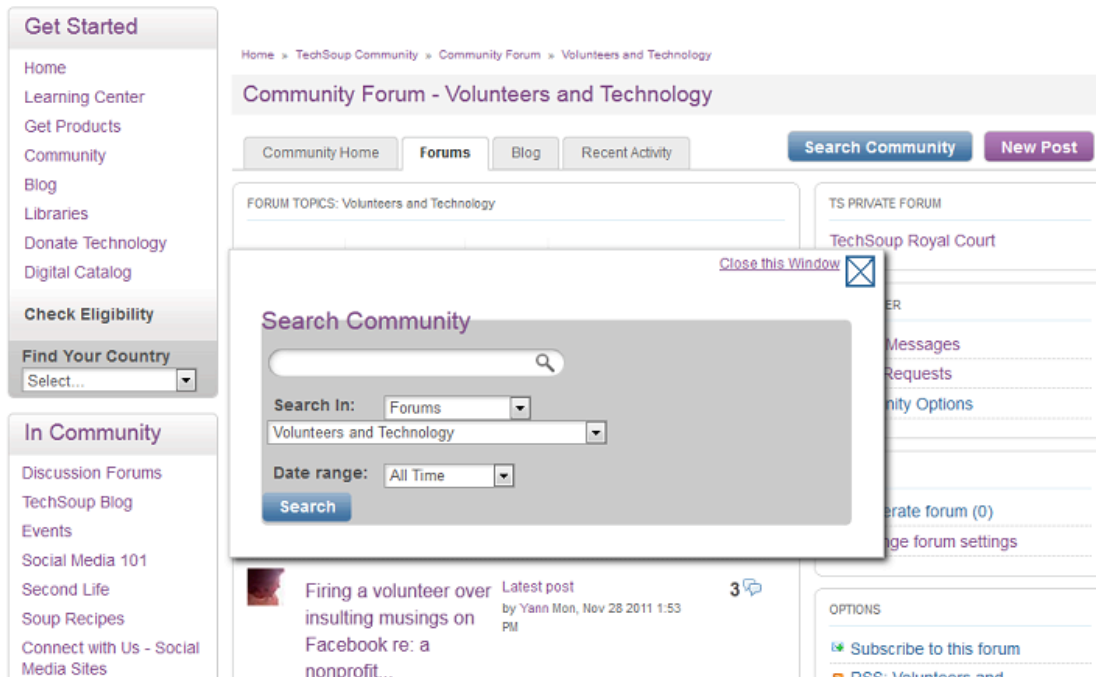
Let's say you have a question about volunteer management software. We've got a category for that! In fact, we have twenty categories, which cover a broad range of topics. The categories are listed alphabetically, so scroll down to the one you want.

Not sure where your question goes? It's okay. Just use your best judgment. If it's misplaced, a friendly TechSoup volunteer host or staff member will find the right place for it.

Virus Vaccination and Computer Security ☆	5650	Tue, Nov 8 2011
Discuss ways to keep your computer secure and virus-free. What do you do when your computer becomes infected? How do you know your computer is infested? How do you keep information secure?		
Volunteers and Technology ☆	1678	Mon, Nov 28 2011
Learn about working with technology volunteers, as well as using computer and networking tech to support and involve volunteers. Also, offer critiques about the volunteer management system you use and your own advice for others.		
Web Building ☆	8523	Today
Strategies and expert advice on all aspects of developing and maintaining an effective Web presence for nonprofits, NGOs, and other mission-based organizations and causes, including web design, SEO, analytics, hosting, and functionality.		
Wireless and Mobile ☆	1816	Mon, Nov 28 2011
Networking Unplugged! Learn and share about using wireless technologies, from mobile phones to wifi. How are nonprofits, NGOs and others using wireless and handheld tech?		

→ Search Community

In the TechSoup forums, we love questions. But before you pose yours, sometimes it's helpful to search the forums to see what other community members have to say. There are years' worth of data on the forums, and many excellent conversations to draw from. Our handy community search features allow you to search all forums, or within a specific forum. Click on the **Search Community** button.



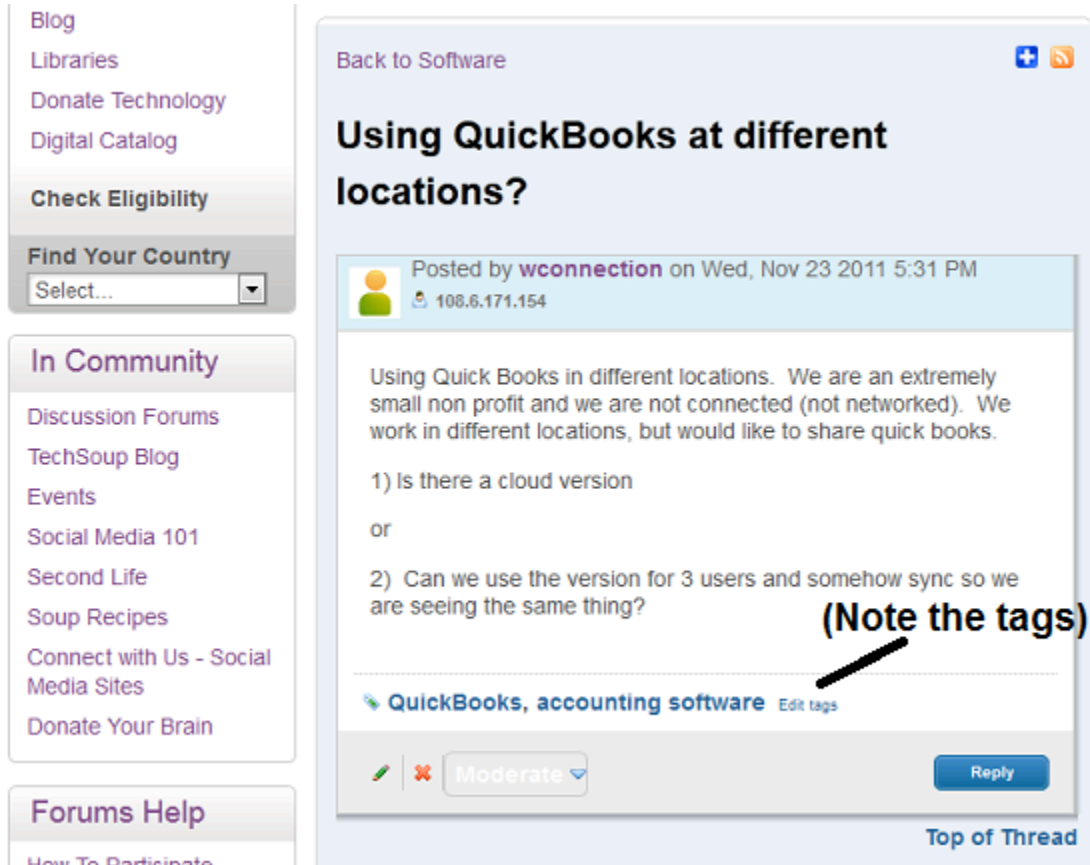
→ How to Ask a Question

Didn't find quite what you were looking for? Ask away!

To ask your question, create a new post as you did in the **Introduce Yourself** forum. To make your post more searchable, you can also add tags to it. This will help future users find the information in your post quickly, and may also help an expert find your question faster. (Experts and forum hosts sometimes subscribe to certain tags in their area of expertise.) Go to the Resources section in this guide for a link to more information about Tags.

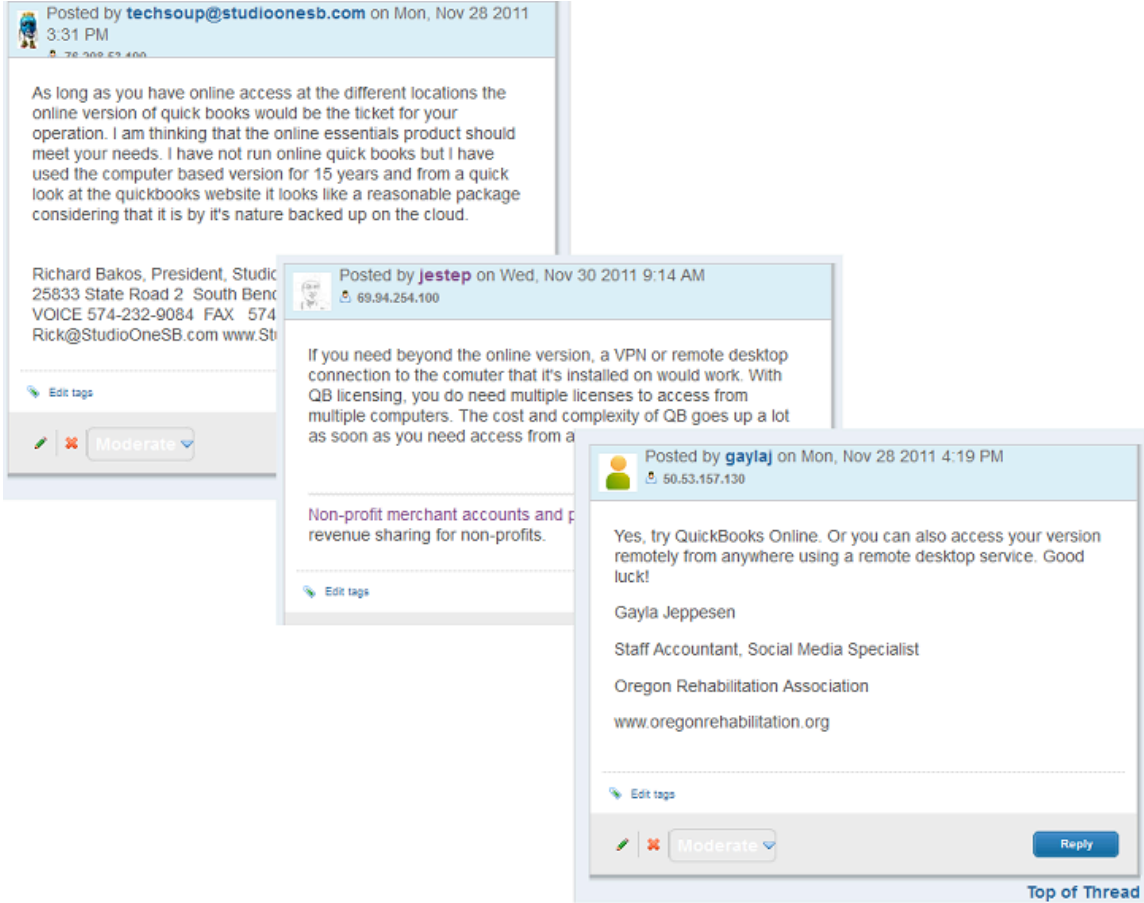
→ Question Samples

Here is an example of how our members ask questions -- and get answers -- on TechSoup. They asked...



The screenshot shows a forum post on the TechSoup website. On the left is a navigation sidebar with links like 'Blog', 'Libraries', 'Donate Technology', and 'Find Your Country'. The main content area features a post titled 'Using QuickBooks at different locations?' by user 'wconnection' on Nov 23, 2011. The post text asks for a cloud version of QuickBooks or a multi-user sync solution. A tag 'QuickBooks, accounting software' is visible below the text, with a handwritten note '(Note the tags)' and an arrow pointing to it. At the bottom of the post are 'Moderate' and 'Reply' buttons, and a 'Top of Thread' link.

And our community answered:



The image shows a collage of three forum posts from the TechSoup Global Forums. The top post is by 'techsoup@studioonesb.com' dated Nov 28, 2011, at 3:31 PM. The middle post is by 'jstep' dated Nov 30, 2011, at 9:14 AM. The bottom post is by 'gaylaj' dated Nov 28, 2011, at 4:19 PM. Each post includes a header with the user's name and timestamp, a main body of text, and a footer with moderation options like 'Edit tags' and 'Moderate'. The bottom post also features a 'Reply' button and a 'Top of Thread' label.

Posted by **techsoup@studioonesb.com** on Mon, Nov 28 2011 3:31 PM

As long as you have online access at the different locations the online version of quick books would be the ticket for your operation. I am thinking that the online essentials product should meet your needs. I have not run online quick books but I have used the computer based version for 15 years and from a quick look at the quickbooks website it looks like a reasonable package considering that it is by it's nature backed up on the cloud.

Richard Bakos, President, Studio One SB
25833 State Road 2 South Bend
VOICE 574-232-9084 FAX 574-232-9085
Rick@StudioOneSB.com www.StudioOneSB.com

Posted by **jstep** on Wed, Nov 30 2011 9:14 AM

If you need beyond the online version, a VPN or remote desktop connection to the computer that it's installed on would work. With QB licensing, you do need multiple licenses to access from multiple computers. The cost and complexity of QB goes up a lot as soon as you need access from a

Non-profit merchant accounts and payment processing revenue sharing for non-profits.

Posted by **gaylaj** on Mon, Nov 28 2011 4:19 PM

Yes, try QuickBooks Online. Or you can also access your version remotely from anywhere using a remote desktop service. Good luck!

Gayla Jeppesen
Staff Accountant, Social Media Specialist
Oregon Rehabilitation Association
www.oregonrehabilitation.org

Top of Thread

How to Get Technical Help

Below are further resources related to participation in the TechSoup forums.

- [More information about filling out your TechSoup profile](#)
- [How to participate](#)
- [Rules and Standards](#)
- [Forum Frequently Asked Questions](#)
- [Tags](#)

If you have further questions, please feel free to contact Michael DeLong, TechSoup Online Community Manager at mdelong@techsoupglobal.org or 415.633.9369.