National
Forum
on Education
Statistics

WEAVING A SECURE WEB AROUND EDUCATION:
A Guide to Technology Standards and Security

NCES National Center for Education Statistics

WEAVING A SECURE WEB AROUND EDUCATION:

A Guide to Technology Standards and Security

Web Standards and Security Task Force

National Forum on Education Statistics

National Center for Education Statistics

Institute of Education Sciences

April 2003

Task Force Members

Acknowledgments

Table of Contents

Executive Summary

The guidebook opens with a discussion of the possible content for web sites at various levels of the education environment. The first chapter emphasizes that the content is the first consideration when the agency decides it wants to build a web site.

Practical considerations necessary for the development and maintenance of a web site are discussed in chapter 2, including the rationale for web publishing standards and guidelines for web site content. Technical guidelines address such issues as password protection.

A web site developed by an education agency will exist within the context of the overall community. Chapter 3 discusses some policy issues to be addressed when considering federal, state, and local regulations. The rationale for having an Acceptable Use Policy (AUP) is followed by a discussion of the relationship between the Internet and existing Open Meeting (Sunshine) laws. Policymakers are encouraged to think about usability guidelines as they relate to federal and state regulations on accessibility, privacy rights, and copyright regulations.

The initial premise of chapter 4 is that any organization can launch a useful web site, no matter what the level of expertise and funding. However, the sophistication of the site and physical location of the web servers will depend largely on where the resources can be found and what funding is available. This chapter delves more deeply into the issues that face an agency as it decides whether to develop and host a web site internally or to outsource the process. The chapter provides some guidelines to assist in selecting qualified vendors for outsourcing and identifies the hardware and software that will be needed for internal hosting and effective use of the web.

Chapter 5 describes the procurement process and outlines three approaches to developing bid requests: (1) technical specifications, (2) request for qualifications, and (3) request for proposals. To help control costs and keep the implementation on schedule, the bid packet should include as much information as the agency can possibly determine in advance. This might include basic design parameters, contract parameters, vendor/contractor qualifications, and any legal issues that might arise. Less specificity will often lead to misunderstandings, delays, and cost overruns. Agencies planning to set up their own Internet nodes or web sites must consider their hardware and software needs, as well as the agency's capacity to maintain the site and train the users of the system.

As the Internet, the web, and other computer applications become more complex, securing the network becomes more challenging. Historically, the Internet has been a magnet for attacks by hackers who find the weak points in a security system and intentionally break and enter into a restricted computer network. Chapter 6 sorts out the complexities of network security and addresses hardware, operating system, and software security protocols. This chapter is intended to meet the needs of more highly technical users. It provides detailed guidelines for securing Internet nodes and networks, including wireless networks. The chapter sections concerning data security and integrity are especially important for district technology directors, who are responsible for the protection of students and the data that relate to students and district employees.

This guidebook builds on, and is linked to, other technology guides developed by the National Forum on Education Statistics (the Forum) and available on the NCES web site:

- *Technology @ Your Fingertips* provides a basic understanding for school leaders of how technology can be used in schools.

- *Safeguarding Your Technology* provides a broad overview of security and the development of security procedures within education organizations.

- *Technology in Schools* helps educators develop procedures for tracking the ownership and use of technology in schools and school districts.

As with other Forum publications, this guide of technology standards and security reflects the "best-practices" judgments of the state and local education professionals and others who contributed to it. The practices endorsed in this book are not required by the federal government, except for any specific citation of law or regulation. The guide is presented as a resource for others to use as a contribution to their own technology efforts.

The Forum documents mentioned above include extensive discussions of professional development for maximizing the use of computer technology in the education community. The professional development sections include recommendations for both instructional and noninstructional staff. *Technology in Schools* even presents suggestions for establishing a computer tracking system for professional development programs.

For readers who want to develop presentations about the topics covered in this guidebook, a PowerPoint® presentation is available at *http://nces.ed.gov/forum*. Agencies may modify the presentation to meet the specific needs of the organization. Additional copies of this guidebook may be downloaded from *http://nces.ed.gov/forum/publications.asp*.

> **Other guidebooks in the Forum technology group are available at *http://nces.ed.gov/forum*.**

Introduction

The World Wide Web (often referred to as simply "the web") has been in existence since 1989/90, a relatively short time, but it is the most flexible and widely used information system on the Internet today. Even without the web, the Internet is useful for educators and students who can use e-mail and are able to transfer computer files from one place to another. However, with the rapid development of the web, the use of computer technology in everyday life has grown immensely, especially in the classroom.

During the initial development and growth of the Internet, access was limited for most students participating in K–12 education. Today, through extensive community support and the federal Education-rate (E-rate) discount program, Internet access is found in nearly every education community in the nation, including rural, urban, and suburban schools.

Teachers and students want the benefits the Internet offers. E-mail has made communication among teachers and students easier to accomplish. Information from libraries and government agencies is widely available over the Internet, and easy to access through the web. As availability becomes pervasive, more people are accessing the Internet. For many community members, it is the main source for information about their schools and local school systems.

Throughout the United States, state education agencies, school districts, and even schools are creating web sites to reap the benefits of information dissemination and exchange. If an educational organization does not have a web site today, parents, boards of education, and even legislators are likely creating pressures to produce one.
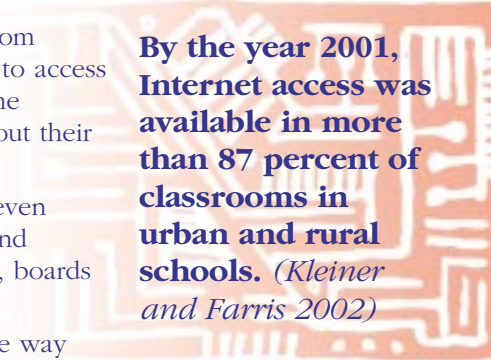
With the growth of the web, the capability now exists for a real change in the way the curriculum is delivered to students. The web has already changed the way information is disseminated within education agencies and the way parents, students, and the public interact with schools.

The purpose of this guidebook is to assist education agencies and organizations (which include state education agencies or state departments of education, school districts, and schools) in the development, maintenance, and standardization of effective web sites. Also included is a detailed examination of the procedures necessary to provide adequate security for the Internet *node* (or connection point) and the network that sends information from computer to computer in the education agency.

Because of the increasing role of the web in education, policymakers today must address many issues that did not exist a few years ago. A knowledge baseline is necessary for these officials and agency staff members so they can make informed decisions about developing and securing computer networks for external Internet access as well as for internal communication.

Educators already understand the imperative of security for students and teachers in the classroom. In this age of technology, security includes the freedom from intrusion via the Internet. Of equal importance is the protection of highly confidential student information and school data from unauthorized access, misuse, or loss, whether intentional or not. For these reasons, this guidebook provides extensive information on procedures for securing hardware, software, and data and for protecting the privacy of students, faculty, and staff.

No single publication will ever be equally effective in addressing the highly technical needs of network administrators and the basic information needs of nontechnical policymakers and administrators. However, recognizing that there is value in having both audiences share a common vocabulary and a basic understanding of the broad vision of Internet use in schools, the authors of this publication have attempted to create a
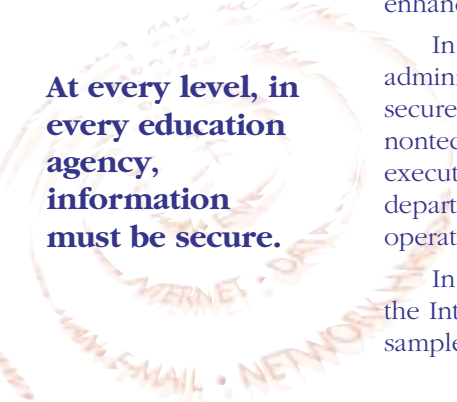
By the year 2001, Internet access was available in more than 87 percent of classrooms in urban and rural schools. *(Kleiner and Farris 2002)*

Who makes informed decisions about an agency's web site?

communication bridge. The first five chapters are intended primarily for administrators. They are written in nontechnical language to address planning, purchasing, policy, legal issues, and the educational value of operating a web site. Technical staff may want to read those chapters to gain a deeper understanding of some of the nontechnical issues and decisions faced by their administrative colleagues. They may also find some ideas to enhance their communication with nontechnical staff members.

In contrast to the first five chapters, chapter 6 is written primarily for network administrators and others who are responsible for ensuring that the agency's data are secure and the equipment operational. Much of this chapter may be difficult for the nontechnical reader, but may provide a second supporting source of information for executive staff when they are faced with requests from an information technology (IT) department for specific hardware, software, and procedures needed to enhance the operation and security of the agency's system.

In addition to an even more basic discussion of how the Internet works (see, "What is the Internet?"), appendices and a glossary provide some useful resources, links, and sample documents that can be modified for local use.

At every level, in every education agency, information must be secure.

The Role of the World Wide Web in Schools and Education Agencies

Introduction

Nearly anyone may have a web site nowadays, from the largest multinational corporation to the family pet. Web site proliferation has influenced public expectations about the role of the Internet in all aspects of life, including all levels of education. Parents and community members today expect to be able to find information on the web about K–12 education in their state, district, and local schools. Many states have even legislated online "report cards" that display a variety of school information such as grades and test scores, discipline referrals, school ratings, and student demographics.

State education agencies, a majority of school districts, and even many schools already have a presence on the web. When parents or other members of the community visit these web sites, they expect to obtain information. They may want to view a school calendar, check on the latest homework assignment, find the phone number for a school board member, or check on school closings. They might go to the state department of education web site for data comparing the performance of a local school or district with others around the state. If the web site is poorly organized or out of date, it reflects poorly on the agency. Today, as technology becomes available to everyone, it is imperative that policymakers pay close attention to their web sites.

Well-designed and maintained web sites can enhance community relations for education agencies and increase their visibility. A more important aspect of the proliferation of this technology is its effect on classrooms and students. A widely held expectation is that every student in the United States will have school-based access to the Internet and, consequently, be able to access the vast amount of information available on the web. Access to the web in schools raises many issues. These include:

- changes in the delivery of the curriculum;
- integration of technology into professional development programs;
- student security; and
- security of critical data.

This chapter discusses some possibilities for web site content in detail. At the outset, emphasis is placed on a needs assessment process as a prelude to the development of a web site.

QUESTIONS ANSWERED IN THIS CHAPTER:

- **Why should an education agency develop a web site?**
- **How does an agency identify needs and resources?**
- **What content might be on a web site developed for schools and districts?**
- **What content might be on a web site developed for state departments of education?**

The Beginning

With pressure to develop a web site, it is sometimes overwhelming to know where to begin. The agency first needs to know the reason for a web site. How will the web site advance the strategic mission of the agency? How will it support the instructional program? How will it improve operational efficiency?

Before assigning the jobs of web development and maintenance, it is useful for an agency to spend time to determine the intended function and content of the site. This initial commitment invariably reduces time spent recovering from mistakes later on. If a web site already exists, the agency may step back and periodically reexamine all aspects of the site and its operation to assure that it is still contributing to the achievement of the agency's goals and objectives.

The Needs Assessment

The needs assessment process should be an outgrowth of the agency's strategic plan that describes the overall goals and objectives of the organization. One of those goals, to establish a web site, is expanded upon as the agency assesses what a web site will do and what content is desired. This process, determining the need, should involve the various stakeholders of the organization.

It is critical to determine what the agency wants to do.

The first issue to address as the agency assesses the need for a web site is the nature of the audience.

- Who are the constituents and what do they need or want to know about the organization?
- Will teachers use the web site for the delivery of the curriculum?
- Are students going to have access to the web site from school computers?
- Will students contribute to the content or management of the web site?
- How will the use of the web enhance interactions and processes?

The agency then can discuss the intended content of the web site. This critical component of site development should not be done in isolation. The quality of the needs assessment will result in a more effective web site development plan.

Web Site Content: Schools, Districts, and State Departments of Education

School and School District Content

Web sites for schools and districts address the general needs of at least five audiences, with considerable overlap among the groups:

(1) instructional content and information for students,

(2) information for parents,

(3) resources for staff,

(4) resources for the board of education, and

(5) information for the community at large, which includes the four previously mentioned constituencies and others.

Instructional content can take many forms. Web sites can be built to contain learning objectives for each grade level, informational databases, and links to other educational web sites or a host of other instructional resources. They can be interactive

sites that allow teachers to create lesson plans that address specific objectives or static sites that permit download of worksheets and completed lesson plans. Many school districts link to state professional development programs delivered over the web.

Access for students will allow a broad range of activities. The web is a portal to research and communication. The web can also act as a "front end" to many instructional applications.

There is a direct relationship between the bandwidth (i.e., the speed of network connection) and the ability of the Internet node and web site to deliver services to the classroom. A site that receives high-resolution pictures over the network requires more bandwidth than a site dedicated to e-mail exchanges or web research. Video requires a great deal more bandwidth than other Internet traffic.

Student and parent information can advise parents and others in the community on what is happening in the school and classroom and can provide resources to assist with the learning process. These resources may be available to the public or, in the most sophisticated sites, may grant password-protected parent access to individual student records. This content may include the following:

- homework information and assistance;
- links to educational databases, online encyclopedias, and other research resources;
- district, school, and classroom announcements;
- student products such as writing samples, art samples, presentations, term projects, and audio/video recordings of student performances;
- school lunch menus;
- school closings for weather and other reasons;
- school safety information;
- school calendar and event lists;
- official communications and handbooks;
- course syllabi;
- school discipline code;
- adopted curriculum guides;
- special education rights, procedures, and other legal information; and
- programs (e.g., gifted) available in the school.

Resources for staff may include the following:

- staff memos;
- professional development opportunities;
- leadership development opportunities;
- online interactive maintenance of professional development and certification records;
- curriculum development plans;
- curriculum maps;
- internal job postings;
- online staff development courses (interactive video) and other live events;
- staff announcements;
- teacher-sharing resources such as sample lesson plans and instructional units;
- links to external teacher resources on the web; and
- e-mail accounts for internal and external communication.
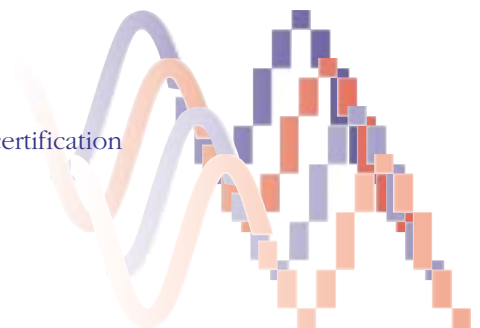
Information for the public is often relevant as well for staff, boards of education, students, and parents. This content may include the following:

- annual reports to the public;
- meeting agendas and minutes;
- policies and procedures;
- employment vacancy announcements;
- employment application materials, either downloadable or interactive;
- athletic schedules, scores, and program information;
- awards won or bestowed by the school or district;
- online surveys and survey results;
- budget information;
- volunteer program information;
- downloadable and interactive forms for a variety of purposes;
- downloadable maps and directions to school/district buildings;
- downloadable or online registration materials for adult education;
- electronic publications;
- staff directories and e-mail links;
- press releases;
- newspaper articles;
- special reports;
- specifications, requests for proposals, and bid results;
- alumni association news; and
- foundation news.

Content for State Education Agencies

State education agency web sites may be more sophisticated than those of schools or districts. As their audience is more general, the content tends to be organized by topic in four categories: (1) information about educational issues in general and the education agency specifically; (2) information about legislation, regulations and standards; (3) information for professional educators about certification, grants, and state reporting requirements; and (4) statistics and information about schools and school districts.

General and agency information may include the following:

- agency organizational information;
- awards;
- budget information;
- catalog of materials;
- downloadable forms for a variety of purposes;
- state education reform efforts;
- electronic publications;
- e-mail links;
- employment vacancy announcements;
- employment application materials;
- events calendar;
- meeting schedules, agendas, and minutes;

- press releases;
- newspaper articles;
- scholarship information;
- special reports;
- specifications, requests for proposals, and bid results;
- staff and program directories; and
- state curriculum frameworks and academic standards.

Legal and regulatory information may include the following:

- charter school approval information;
- notices of agency rulemaking and hearings;
- state textbook adoption information;
- state curriculum standards and curriculum frameworks;
- agency policies and procedures manuals; and
- testing and graduation standards.

Information for schools, school districts, and professional educators frequently includes the following:

- downloadable or interactive grant applications and supporting materials;
- links to other education resources;
- official communications;
- online staff development and other streaming video events;
- reporting cycles and due dates for state reports; and
- teacher certification requirements, applications, and other information.

Statistical and descriptive information on individual schools and school districts is frequently reported on the state agency's web site. This content may include the following:

- downloadable maps and directions to school/district buildings;
- links to school/district web sites within the state;
- school/district profiles and performance reports;
- school approval (accreditation) status;
- school construction information;
- special education information; and
- state directories of school/district contacts.

Summary

- The first step in building a web site is to conduct a needs assessment.
- Stakeholders need to be involved in the needs assessment process.
- Web content will vary according to the audiences the agency wants to serve.
- School, district, and state department of education sites will have different content.

Web Publishing Guidelines

Introduction

Because basic web sites are not difficult to program, schools and individual students are creating their own Internet sites. Since any site associated with an education agency will reflect on that agency, it is important to develop policies that will ensure consistency, while not stifling creativity. This chapter discusses the guidelines an agency should consider to present a functional site that reflects its mission. Guidelines might include who will decide the content on the site, the "look and feel" of the site, and what procedures will be in place for updating and making changes.

Guidelines that incorporate procedures and regulations in the areas of *content, technology,* and *usability* are effective in developing a foundation to maintain an effective, user-friendly, and secure site. Education agencies need to be aware of privacy rights, factors that affect how web pages are displayed by different browsers, and especially the many security issues related to Internet and web access in the schools. Agency guidelines should be made available to the people who develop or post content to the site.

QUESTIONS ANSWERED IN THIS CHAPTER:

- Why does an agency need web publishing guidelines?
- What are content guidelines?
- What might an agency examine when considering advertising that is available on the web?
- What technical guidelines are useful when developing a web site?

Content Guidelines

Many times, the first impression the public has of an agency is its web site. In addition to reflecting the agency's mission and containing appropriate and useful content, the site should be attractive and well organized. A district, for example, may decide to include a page on its web site about employment opportunities. If the application procedures on the site enhance the ease of applying and contain useful information about employment in the district, the site may help the district attract new teachers. A disorganized web site will likely create a poor impression of the district and may turn prospective teachers away.

Regardless of the sophistication of the site, basic rules apply. First, the site should be organized so that a novice can navigate easily from one section to the next. A good rule for any but the most extensive sites is that the user should be no more than two clicks away from any important information. Links to other sites should be clearly marked. Clean, individual pages should be designed; a cluttered screen makes it difficult to find the content. Each page should be checked periodically to ensure that all graphics are loading properly and that all links are active. If the organization does not have the resources to support a sophisticated site, it is better to start with a simple site that can be kept current and operational than to have a site filled with "under construction" graphics and/or outdated information.

In many cases, education agencies perceive the web site primarily as a vehicle to inform personnel and the public about their activities and goals. There are other reasons, including the delivery of instructional content, for establishing a web presence. To administer the content on the agency's web site effectively, content policy and procedural guidelines should be established as a component of the agency's technology plan before moving forward with web site development.

Guidelines for Posting New Content

Build on a simple start. Prepare for the future.

The first step, before any programming begins, is to determine what the agency needs and wants the web site to do. Beautiful sites can be created with flashing icons, dynamic colors, and interesting text. However, if the content does not meet the needs of the agency, the value is, at best, limited.

Everyone has visited a web site where navigation is impossibly difficult, where one has to spend a great deal of time "clicking" around the site, or where links to other sites do not work. Without guidelines and a quality control process, problems like these are inevitable.

The agency should develop a clear process for deciding what and how new materials are posted to the web site, including whether an approval procedure is needed for new sites and pages. The procedure may be as simple as a request for space on the agency's server, or it may be a more complex approval process involving a committee review.

It is important for the agency to distribute the guidelines for posting new content and to make sure that staff are aware of the process. Posting the procedures and content guidelines on the web site for easy access can accomplish this task. Additionally, it is imperative that the staff understand the procedures and guidelines.

Local coordinators and students may develop some of the most innovative school web sites in-house. While the agency will want to support such innovation, guidelines need to be followed in all areas of site development. As the district is ultimately responsible for the content on school web sites, it may be in the district's best interest to have a representative (e.g., a school site coordinator or webmaster) at each school who understands and is able to support district guidelines and regulations.

Where the district is unable to assign a site coordinator or webmaster, every effort has to be made to ensure that there is a person familiar with district guidelines and other regulations at each location where content may be posted.

What Should the Content on a Web Site Look Like?

The web site design should present a consistent look and feel for a sense of continuity across a site's pages. One way to accomplish this is with the use of style sheets that are embedded or linked to the site within the programming design. Style sheets, or templates, define the format for each page in terms of such elements as typeface, margin width, heading specs, spacing, and layout.

This does not mean that all pages need to look the same. Not all web pages on a site will use style sheets. The purpose of style sheets and other formatting tools or guides is to create consistency, not stifle creativity. However, each style sheet should contain:

- a *home* button that returns the user to the agency's home page with one click of the mouse;
- the name, address, and telephone number of the agency;
- the agency's webmaster's e-mail address;
- copyright notification; and
- a privacy statement.

Advertising on the Agency Web Site

The agency should address the issue of advertising on the web. Advertising of products is allowed in some schools and districts; for example, at athletic events. Other agencies do not permit advertising. Policy decisions regarding web site advertising should be consistent with other agency policies regarding advertising.

Agencies should be wary of Internet service providers (ISPs) that offer "free" disk space, or other services, in exchange for the right to display advertising on the site. Some of these services will run banner advertisements or pop-up ads while the user (in the school's case, a student) is online. Some ISPs even profile users and sell their names and access information to other service providers or advertisers. While this process is commonplace on the Internet, it may be inappropriate for school or district sites.

What does "free" really mean?

Some agencies have determined that it is in the best interest of the students and staff to limit web site access to government and other research sites that do not carry any commercial endorsements or allow "pop-up" advertising. This is accomplished by using a program to filter (see Chapter 3) out unwanted sites.

Situations exist where the vendor who programmed the web site or the donor who funded the web site programming might request that the agency place an "icon" on the home page of the web site to advertise their contribution. If the agency agrees to place an icon of this type on the web site, many more requests may follow.

Agency Web Site Disclaimer

A disclaimer statement should appear on the agency's web site acknowledging that the public has the freedom to browse the site. The statement should include information about copyrighted material and may include language disclaiming responsibility for some Internet activities. The agency should consult with its attorney about the specific language and content of the disclaimer. To view an example of a web site disclaimer, visit West Virginia's State Department of Education site at *http://wvde.state.wv.us/disclaimer.html*.

Allocation of Space, Maintenance of Files, and Web Development Policies

Technical Guidelines

There are several technical guidelines the agency should employ when web pages are created. If the agency's web site is to be maintained and updated by more than one person, an established set of procedures for accomplishing these tasks will assist in ensuring dependability and consistency. The technical guidelines developed by the agency can serve as the procedural handbook for implementing policies governing web use. Aspects to consider when developing technical guidelines include:

Create consistency by establishing procedures for changing web sites.

- compatibility of guidelines with recent releases of the major web browsers, as well as with older browsers;
- optimization for different web browsers;
- load time of the web site using a variety of modem speeds;
- use of approved file extensions and directory structure;
- use of an Internet-friendly color palette (see chapter 3, "Accessability Guidelines");
- content of meta tags—information inserted into the "head area" of the web page—to improve access to the agency's web site by search engines from outside the agency;

- removal of unnecessary HTML tags;

- use of standard navigation bars and icons throughout the site; and

- determination of whether to use, or prohibit, frames.

Contractors who develop sites for educational agencies should be subject to the same organization guidelines concerning web site development as would an in-house developer. While a contractor may be able to select appropriate technical guidelines, the organization still must be responsible for content, accessibility, and style. Accordingly, there should be clear standards and procedures in place when the contractor is selected, and the contractor should agree to abide by all of the standards before the organization signs a contract.

Password Security

Don't tape that password to the keyboard or onto the monitor!

The use of passwords is important for securing the privacy and confidentiality of student and personnel information. Passwords can also assist the agency in monitoring access to mission-critical applications. All agencies that maintain a web site, including schools, should consider policy issues related to password security. These procedures should be written and distributed to all members of the agency.

Some password-related issues include the following:

- A password should consist of both alpha and numeric characters.

- The agency should require that passwords be of a sufficient length (e.g., eight alpha and numeric characters).

- The agency should establish procedures that require passwords to be changed frequently (e.g., every thirty to sixty days).

- Passwords should not be shared or "loaned" to another person.

- Passwords should not be written down.

Password security procedures should include a help desk, or an automated process, for staff to contact when a password is forgotten. Password restoration procedures should include a method to verify the identity of the person calling the help desk. This could include recalling the staff member's social security number, mother's maiden name, or some other item that will identify the person requesting a new password.

Summary

- Agencies should establish guidelines for posting content on a web site.

- Web site content guidelines should address consistency without stifling creativity.

- Agencies should develop procedures to deal with advertising on the Internet, especially if the agency uses an outside ISP to host the web site.

- Technical guidelines are necessary for password protection.

Web-Related Legal Issues and Policies

Introduction

There are some aspects of web development necessary to meet federal, state, or local laws and regulations. Many of these regulations are adapted from rules or laws that existed before the advent of the Internet. For example, education agencies have long been required to comply with copyright regulations, Sunshine Laws (see below), and student privacy rights. New technologies mean that new procedures may need to be in place.

An Acceptable Use Policy (AUP) should be developed by an agency that allows students, staff, or community members to use computers or to connect to the Internet through the agency. The intent of an AUP is not to exclude anyone from using a computer, but to be certain that everyone understands that this usage is a privilege that can only be retained with appropriate usage.

This chapter concludes with a discussion of Internet filtering. For example, should an agency or school filter out web sites that may be objectionable? This chapter does not attempt to answer this very difficult question definitively. Rather, it describes various filtering techniques that could be employed.

Internet Usage

At the same time an agency is deciding on content for a prospective web site, agency staff should think about related policy issues and guidelines that will affect the entire organization. Even though the World Wide Web has been around for a relatively short time, the Internet has been in general use long enough that effective practices already exist based on well-known pitfalls. Now is the time, if the organization has not done so recently, to review Internet policies and procedures.

Many of the needed policies, such as *"acceptable use"* and *"right to know,"* have legal implications and may be required by local, state, or federal regulations. This chapter provides general guidelines for awareness of potential legal issues, but does not purport to give legal advice. Specific legal questions should be discussed with the agency's attorney.

While many school districts and state departments of education are attuned to the need for many of the policies and guidelines described below, the school technology coordinator and/or the students creating the school web site may not be aware of the policy issues that arise when a web site is developed. The district is ultimately responsible for its school web sites and must ensure that each school adheres to applicable laws and regulations.

QUESTIONS ANSWERED IN THIS CHAPTER:

- **What is an Acceptable Use Policy?**
- **How do state "Sunshine Laws" apply to web communication?**
- **When should an agency filter its web site?**
- **What are some legal issues to be addressed?**

A district is responsible for a web site developed at a school.

Acceptable Use Policies

Whether an organization provides direct services to students or serves as a support or regulatory body for schools, adoption of an AUP is essential. The purpose of this policy is to inform users of the ground rules, thus protecting them and the education agency from violations of law, practices that would damage the system, or misunderstandings regarding who is responsible for what.

The responsibility of "acceptable use" comes with the privilege of Internet access that is afforded to students, staff, and, sometimes, parents. No one should be using the Internet in a school or district environment until that person has reviewed and signed the agency's AUP. Where students are concerned, parents need to review the AUP and complete the signature page, indicating their understanding.

An AUP should include the following:

- notice of the rights and responsibilities of computer and network users;
- notice of legal issues, such as copyright and privacy;
- notice of acceptable content and conduct on the network;
- description of behaviors that could result in disciplinary action; and
- description of the range of disciplinary options, including the removal of access privileges.

The AUP applies to all users accessing the Internet from agency terminals or computers. This includes teachers, students, parents, and other members of the community who might use the Internet at an agency site. For example, members of the community using school computer labs to learn about technology also need to review the agency's AUP.

The AUP should be available in a variety of formats for those who do not speak English or who have a disability that makes reading the policy impractical. Finally, the agency should avoid including provisions in the policy that it is not willing to enforce, or that will create difficult legal situations by their enforcement. All users need to understand the consequences of failure to comply with the AUP.

Each AUP should include a detachable page where the user, or the parent or guardian of a student, can acknowledge that he or she has received, read, and understood the policy. The agency should retain this sign-off sheet. No student should have school-based Internet access without specific written approval of a parent or guardian. Parents need to work with agency personnel to ensure that students understand the components of the AUP.

An example of an AUP along with a parent signature sheet and other policy documents are provided in appendix E of this document.

Open Meeting (Sunshine) Laws and the Freedom of Information Act

Every state has some version of an open meeting law, frequently called the Sunshine Law or Right-to-Know Law. The intent of this type of statute is to ensure that public business is conducted openly and that access to public records is guaranteed to the citizens of the state.

Many of these laws have not been updated to recognize electronic communication; however, this has not stopped courts from applying the laws to such communication. To avoid problems that might arise, if a public agency maintains a web site, an e-mail server, list servers, or electronic bulletin boards, policies should be in place to address the use of

> **Internet usage for staff and students is a privilege, not a right.**

> **A student should have specific written approval of a parent or guardian for school-based Internet access.**

these media for communication among the members of a governing body, such as a board of education.

Use of electronic media to inform public officials and the public generally is not contrary to law. However, in many states, when the communication invites, or results in, responses from and discussion among public officials, such communication may constitute an illegal meeting. Some states' laws specifically prohibit electronic meetings. Others, while not prohibiting such a meeting, may require public notice stating that the meeting will occur and identifying a location where the public, in real time, can monitor the electronic communications.

Electronic files are subject to the same legal requirements as paper documents.

Under the Freedom of Information Act (FOIA), members of the public can request, and must be granted access to, any documents in the possession of a public agency that address public business and are not specifically protected by other statutes establishing classes of confidential records. Over the years, public agencies have developed records retention policies designating how long their paper documents will be retained in the files before disposal or destruction will be permitted. Under FOIA, electronic files are subject to the same legal requirements as paper documents, so it is important for an education agency to maintain an archive or archives of e-mail and other electronic documents as they would paper documents.

Usability Guidelines

Simply stated, usability guidelines ensure that visitors using various software packages are able, optimally, to view a web site. For example, programming requirements for Microsoft's Internet Explorer® are somewhat different from those for Netscape. In order to accommodate users of both applications, a web site has to be programmed accordingly. While there are no legal requirements to accommodate users of different software applications, agencies should consider the issue and establish formal guidelines.

Certain aspects of maintaining a web site, such as *accessibility, privacy,* and *copyright*, may require compliance with laws or federal regulations. Whether working with outside sources on the development and/or maintenance of the web site or managing the process in-house, the agency needs to have policies in place to ensure that usability guidelines are followed.

Accessibility Guidelines

The World Wide Web Consortium (W3C), an international group seeking to optimize the use of the web, has developed standards to address Section 508 of the Rehabilitation Act [29 U.S.C. 749d] requirements (see appendix F). These standards, known as the Web Access Initiative (WAI), provide practical guidance for web developers in designing accessible web pages. The standards are prioritized and include sample HTML programming code to assist developers.

Web sites are effective tools to assist people with disabilities.

Web site accessibility measures include the following:

- Attach alternative text tags to graphics. The tags can be spoken to visually impaired and blind users with programmable screen readers.

- Avoid the use of red and green in web text. Use of style sheets to set standard color schemes on a web page will permit color-blind users to modify colors easily from within their own browsers.

- Enable synchronized captioning of audio files and avoid the use of streaming audio for deaf and hearing-impaired users.

A free service for checking web site accessibility according to WAI and Section 508 standards is located at *www.cast.org/Bobby/.* For more detailed information about W3C and WAI guidelines, visit *www.w3.org/TR/1999/WAI-WEBCONTENT-19990505/.*

Student Rights and Privacy

The Family Education Rights and Privacy Act (FERPA) regulates the dissemination of student information. The regulations apply to information posted on the Internet or web. The posting of student work, photos, or other personally identifiable information on a web site is one of the most obvious issues addressed by federal and state privacy laws.

One might ask: If the Internet and World Wide Web are used to access information outside an agency, how can internal privacy issues be a concern? Often web sites are created to inform the community about the activities of a district or school. Under these circumstances, classroom or schoolwide test scores may be displayed. These web pages may be based on student databases that are maintained by the agency.

Student privacy is an agencywide issue. Even computer programmers need to be trained on the provisions of federal, state, and local laws and regulations that prohibit the display of individual student information, particularly when such information exists in agency databases.

Even if a district does not maintain a database of *all* students, there is a great probability that databases of special education or Medicaid-eligible students exist. Such databases would be subject not only to the privacy requirements of FERPA [20 U.S.C. 1232g] but also the privacy regulations of the Health Insurance Portability and Accountability Act of 1996 [45 CFR Parts 160 and 164] (HIPAA) and the Individuals with Disabilities Education Act [20 U.S.C. 1400 *et seq.*] (IDEA). In addition to protecting the privacy of students, agencies maintaining databases must provide security for employee records as well.

Discussing laws and federal regulations about student privacy may seem esoteric, or even unnecessary. However, it is not a difficult task for a person to make contact with students simply by using information obtained on the Internet. While this may be a frightening scenario, a photograph connected to a name displayed on a school web site makes it much easier to identify a student.

Policymakers are urged to provide this guidebook to their district information or technology director or their school site technology coordinator for a review of the information in this chapter and the discussion of security procedures in chapter 6. Additionally, the federal acts named above should be reviewed.

> **People should not be able to identify individual students from an agency web site.**

Copyright Compliance

Many educators have common misconceptions about Fair Use Doctrine for schools and libraries under the United States Copyright Law [17 U.S.C. 107 *et seq.*]. This misunderstanding, coupled with a general belief that anything found on the Internet is free for the taking, can put the agency at risk of severe legal penalties.

Establishing a link from one web site to other web sites is entirely within legal practice; however, copyright law protects the materials on those web sites. It is imperative that educators have a reasonably good understanding of what constitutes "fair use" and what is prohibited. The education agency's policy and its accompanying procedures should provide guidance to users and should establish, without equivocation, that violation of copyright law is contrary to the policies and practices of the agency.

Copyright compliance applies as well to the use of the Internet by students. For example, it is important for educators to ensure that students understand fair use of citations and quotes obtained online for use in their own class presentations and reports.

> **Student reports must cite information gathered from the Internet the same way information from other media is cited.**

Filtering

Filtering is required if the agency has benefited from discounts for internal school connectivity or Internet access via the E-rate discount program. See *http://www.sl.universalservice.org* for up-to-date E-rate information.

Filtering of Internet content is one of the most controversial issues facing schools and districts using the Internet. Proponents of filtering are concerned about protecting children and teens from inadvertently, or intentionally, visiting sites with pornographic material, hate group rhetoric, or other inappropriate material. Opponents believe that censorship of any kind, even for children, sets a dangerous precedent that is contrary to the free speech provisions of the U.S. Constitution.

For schools and districts participating in the federal E-rate discount program, the question of whether to filter is answered by provisions of the Children's Internet Protection Act (Public Law 106-554). This act, often referred to as CIPA, requires agencies receiving E-rate discounts for school connectivity or Internet access to employ a filter, regardless of their philosophical preferences.

There are many options available for agencies that choose, or are required, to place some type of filtering system on their web site. All methods should be considered carefully to determine what they do, how they operate, and how much time the agency will need to devote to maintaining the filtering system.

The earliest filtering programs still in common use contain lists of keywords or phrases likely to be found on objectionable web sites. These lists tend to be static and inflexible. The primary complaint about this type of filter is that it blocks access to a large number of appropriate sites, such as those describing research on breast cancer and government data files listing the data element for gender as "sex."

Whether to filter is not as straightforward a decision as it might appear.

An alternative to the list filter is a subscription to a service that constantly reviews and screens new sites for objectionable material. Specific sites, rather than words and phrases, are blocked. The main objection to this method of filtering is that access to some objectionable sites is still possible because monitoring every site on the Internet is impracticable. A newly emerging challenge for filtering services is the purchase, by "disreputable" companies, of Uniform Resource Locators (URLs), or web addresses, previously owned by other businesses and organizations. These URLs are used to mask the true nature of a site.

Most subscription lists accommodate manual overrides to permit the local network administrator to define trusted and questionable domains. Reviewing lists to determine what the filter should override is a time-consuming process and, therefore, expensive. Generally, it is impractical for an organization to structure its entire filtering system on this basis.

A larger agency may choose to develop its own process for filtering the Internet. While providing more flexibility for the agency, this effort can be resource intensive. Personnel will need to be assigned to determine which sites should be filtered. The agency will need to establish procedures for monitoring the filter and for responding to requests from staff to modify the filtering protocol.

In addition to filtering content and advertising, the agency may consider filtering unacceptable services. For example, it may block "free" web-based e-mail services, instant messaging services, or chat rooms. The agency may additionally choose to block the downloading of multimedia content, such as music files or movies, because of its heavy use of bandwidth and copyright issues.

Within the local network, the agency may have the ability to restrict Internet access on specific computers or work groups, while granting broader access to others. Thus, a filter may be active on the firewall for computers used by students but configured to grant greater freedom to faculty or administrative staff computer users.

Many districts deal with filtering and web-based advertising proactively. They filter *all* sites and then determine which sites would be appropriate for use within the agency. Students are allowed access to approved sites only.

Agencies discussing a software or hardware solution with vendors should ask about the criteria used to determine what is to be filtered. If a vendor has a specific political or moral agenda, for example, sites may be filtered that oppose that agenda.

While there is a great deal of discussion about filtering out inappropriate sites on the Internet, there is no substitute for the vigilance of teachers. Professional development programs should stress that *surfing* the Internet is an inappropriate activity for students at school. The web, in a classroom, should be treated as an instructional tool, not a plaything. The agency's AUP should contain language that defines the appropriate use of the Internet by students (see appendix E for a sample AUP).

Logging System Usage

Even if an agency does not require filtering, the related issue of access to and maintenance of Internet logs must be considered. The logs are electronic records documenting the sites visited from the agency's network. One New Hampshire parent successfully sued a school district to gain access to its Internet logs in order to determine whether the district, which was not filtering, was providing enough protection to students through its AUP. The judge granted the parent's request for access, but the district had already deleted the logs.

In addition to the question of access, the district found itself having to defend its position related to the deletion of the records. The problem was not just that the records were deleted, but that there was no policy governing a file maintenance schedule or purging procedure. In short, because the district had no standard operating procedure in place, it appeared to the judge that the logs were deleted to prevent their use as evidence in a legal action. The court found the school district to be in contempt of court and ordered it to produce the remaining records and to pay the parent's costs and attorney's fees. The case could set a precedent regarding parent access to logs that will affect schools and districts nationwide.

The bottom line is that a policy must be in place regarding the retention and destruction of files and must address the use of all computer systems within the agency.

Summary

- A district is responsible for a web site that is developed at a school within that district.
- An Acceptable Use Policy should be available for all users of the Internet within the agency.
- The Freedom of Information Act and state Sunshine Laws have an impact on the use of the Internet in an education agency.
- Usability standards can be employed to ensure that the web site has the widest possible audience.
- Student rights and privacy guidelines that apply to the education community include the use of the Internet and its components, such as the World Wide Web.
- Usability guidelines must address access for individuals with disabilities and the protection of privacy and confidentiality rights of students.
- There are many options available for filtering web content.

Internal and External Resources for Web Development

Introduction

Once the agency has determined that a web site will serve a useful purpose, staff will need to determine how the web site should be built. The needs assessment process will help to determine if resources exist within the agency to match its needs. One goal of this exercise is to see if the site should be created in house or whether web development should be outsourced (developed by an outside company). Additionally, staff will need to determine if the new web site should reside, physically, on servers owned by the agency or if an outside vendor should be hired to house and maintain the web site on its servers. Agencies with existing sites may want to revisit these issues periodically in planning for the maintenance and upgrade of their sites. Agencies need to know if expectations based on an assessment of the needs of the agency match the ability to meet them.

Needs Assessment Checklist

One purpose of the needs assessment might be to determine if the agency has the ability to support a web server, portal, and computer files on its own. The following questions should be considered:

- Does the agency have funds for servers and the appropriate space to house the servers?
- Does the agency have staff available to maintain the servers?
- If staff are available, what additional training will be needed to maintain the servers?
- Should web content management be centralized or decentralized—that is, will one person/department manage the entire site or will each department manage its own section?
- What web design skills are on staff?
- Once the major development is complete, can the existing staff support the system?
- Will instructional applications be delivered over the web site?

The degree of difficulty in programming grows with the complexity of the web site. Some sophistication is required to build and maintain a web site that, for example, accesses databases containing student assessment scores and develops methodologies for making comparisons of student success rates. Templates can be used to set up a web page or web site, but more knowledge is needed to develop a graphic design motif that will be used to represent the agency on the World Wide Web whenever anyone visits the web site.

QUESTIONS ANSWERED IN THIS CHAPTER:

- **Do the needs of the agency match the available resources?**
- **How should agencies determine whether to outsource or develop web sites in house?**
- **How does professional development fit into agency plans?**
- **What software could be employed to implement the web site?**

Just as a computer needs software for people to use it, a web site needs applications. These applications provide the tools that make the World Wide Web valuable to educators. Additional applications are necessary to protect the web site and the data that may be accessed through the web.

Identifying and Matching Available Resources to What is Needed

Deciding what to include on the organization's web site is influenced as much by the expertise and resources available as by the desire to provide specific content and services to constituents. At the most basic level, there are vendors able to provide a service that enables teachers and others to post, in a simple format, information about homework, class activities, and a host of other items. A fee may be assessed for the service or access may be free if advertising is allowed on the agency's web site.

There are Internet Service Providers (ISPs) that provide templates for novice programmers. These templates require simply that the individual posting the content visit the site with a password for access and then "fill in the blanks" to create web pages.

A school or district with little expertise and limited resources may choose to set up a small web site offering basic information to staff and the community. The site may be limited to information that does not change often, thus requiring infrequent updates and little maintenance. High schools often allow students with enough expertise to help manage the design and content of these basic sites at little or no cost to the school and with minimal time commitment from staff.

A small district, or school, may decide to outsource many aspects of web site support. A major advantage of this plan is that a local ISP can keep the small district web site operational 24 hours per day without making demands on district resources. However, the agency should consider that, often, a basic service plan provides little disk space for expansion and few options, if any, for a database or other interactive features. Additional features and the required technical support may be available for an additional fee.

A larger district with more funding and on-site technical staff may choose to manage every aspect of a complex web site, including databases, interactive pages that allow remote data entry by site visitors, and other advanced features. State education agencies typically operate their own sites and employ technicians to keep the site operational and the pages up-to-date.

There is a middle ground. There are ISPs that will provide any of the services that an agency requires—for a fee. As with most endeavors, careful planning can make all the difference. A needs assessment resulting in a coherent plan will enable web site development and implementation to progress smoothly and provide better results. This is true whether starting from scratch or modifying an existing site.

To Host or Not to Host– That is the Question

The *host* of a web site is the agency or company that operates the site on a web server. Using an outside hosting service allows many companies to share the cost of a fast Internet connection for serving files. Ultimate control of the web site, however, is achieved when the agency operates its own server.

Little expertise is actually needed to launch a web site, but considerable knowledge and resources are required to operate web servers. States and large school districts may find that hosting their own web sites is the most effective way to enhance their sites with

interactive features, such as form submissions, discussion groups, e-commerce, job applications, and customized content delivery for the instructional program.

An organization should consider in-house operation of a web site if the necessary expertise and budgetary resources are available to ensure proper functioning. However, schools and districts can unknowingly expose themselves to serious problems if they do not have properly trained network administrators and support staff. For example, during the preparation of this guidebook, one of the writers came upon a school district web site that inadvertently allowed open access to everything on the district's main server, including access to student records. Properly trained staff would have the technical expertise to prevent such a situation from occurring.

Outsourcing Web Site Development and Maintenance

Along with determining where the web site will physically reside, the agency needs to determine who will design the look and feel of the web pages and who will write the programming code. In many small schools or districts, the web site might be the outgrowth of a single workshop attended by a teacher or a student who has an interest in technology and wants an opportunity to demonstrate his or her skills. Such sites generally start out as basic, static files, frequently without a coherent plan for content selection, file management, or publishing standards.

When resources are not available in the agency, outsourcing the development and management of a web site might be advisable. In some cases, outsourcing can provide a more sophisticated design and more efficient file structure, leading to a higher level of reliability. Because a successful web site attracts more users, web site management should include constant monitoring of the equipment and operation to track site usage in order to identify a need for upgrades. Commercial ISPs are often better able to cover the cost of upgrades for speed and data flow by spreading that expense among their clients.

Outsourcing web development can also give smaller organizations access to highly qualified teams of graphic designers, who can create customized graphics, and programmers, who can write code specific to the organization's needs. Without programming expertise, the organization is usually limited to standard features available in off-the-shelf web design programs. Many of these programs include powerful design options; however, a web design novice may not have the knowledge to apply the full power of the program to optimize the site's speed, graphic quality, and storage space efficiency.

Size is not the only factor in the decision to outsource. Even for smaller districts with few resources, there are situations where outsourcing will not be desirable. In some situations, small, simple sites with static pages may be more appropriate for the school or district than professionally designed sites that will require constant maintenance. As a site becomes more complex, the need for professional help will probably become apparent, and the cost of development and maintenance will increase accordingly. If in-house design and development are considered, it is also important to consider the cost of the superintendent's or school principal's time if he or she is required to work with an amateur web developer.

If an agency does not have full-time information technology (IT) staff members to devote time to web maintenance, a paid contractor may be necessary. A carefully selected contractor, with the appropriate software and knowledge, can track site activity and make changes in an efficient and consistent manner.

Combining Outsourced Services with Internal Resources

The needs assessment often will reveal that an agency has the resources needed for some but not all aspects of connectivity, web design, and server maintenance. For some agencies, it may be more effective to outsource specific tasks, such as initial design and programming, then to transfer management and maintenance to internal staff.

Using outside personnel and equipment at the beginning may buy the agency time and experience, allowing staff to become familiar with web site support. When adequate internal support is possible, the site could be moved onto agency servers and supported by agency personnel. As the complexity of the web site grows, the agency will know if it has the resources to meet the expanded needs.

Because of the nature of web design, it is not necessary for the designers to be physically present on site. Unless state or local policies favor hometown businesses, selection of vendors for web site design, development, and operational services typically draws from a nationwide pool. While this gives the education agency access to a higher level of expertise and a broader range of choices, it also increases the probability that proposals will come from unknown companies or individuals. If any portion of an agency's web site development is outsourced, it is critical that the agency develop a Request for Proposal (RFP) that clearly defines the needs of the agency and the parameters of the contract.

Outsource some services. Keep others inside the agency.

Training and Professional Development

The need for professional development for effective Internet use within an education agency goes beyond training for developers and programmers. All staff members and student users of agency equipment need to have an understanding of the policies governing its use and enough technical skills to navigate the web and use other appropriate computer applications. Because technology changes so quickly, continuous training is helpful for users and is essential for those who maintain and operate the network. Budget allocations should address training and technology-related professional development as a necessary component of the agency's overall program.

Professional development for teachers goes far beyond training in the use of the computers, the Internet, and the World Wide Web. Technology will not be integrated successfully into the school environment until teachers are able to integrate the technology into their curriculum delivery process.

This guidebook does not contain a detailed discussion of professional development for teachers in the integration of the web and other technologies into the curriculum; however, this does not minimize the need. Other Forum publications, such as *Technology in Schools* and *Technology @ Your Fingertips,* discuss professional development procedures at greater length.

Internet-Related Software

Software makes the hardware work.

One of the many decisions an agency must make when considering web site development is what software to include. These choices may have an impact on the decision whether to outsource the programming, server storage, and maintenance of the site or whether to host the site in house. Agencies with the sufficient resources to maintain secure servers in house should consider the following software needs before making related purchases.

Browsers and Acrobat Reader™

Two basic pieces of software are essential for reading and downloading files from the web. One is the Internet browser. Nearly all computers purchased include browser software, which permits the user to access and display Internet-compatible graphics and text contained in files written with hypertext markup language (HTML), Active Server Page (ASP), Java, or other Internet languages. Simply stated, the browser is the software that allows the user to use the web.

As the features available in Internet files change from year to year, the browser capabilities and associated *plug-in* software needed to take advantage of the new features also change. Most browsers offer free upgrades, which can be downloaded from the Internet. It is generally desirable to upgrade the browser software on computers from time to time, so the browsers will operate efficiently with available file types and features.

Some agency-specific programs, such as student information systems and financial packages, are accessed using a web browser. In these situations, it is not advisable to permit upgrades to browsers unless the technology staff can be certain the applications will run on the new browser upgrade.

A browser is designed to access and save web pages; however, not all pages are easily printed or can be viewed in their original format. The second essential piece of Internet software, Adobe Acrobat Reader™, reads documents that have been transformed from a multitude of word processor, spreadsheet, database, and other file formats into a standard Portable Document Format (PDF). The software enables the computer to display the file in its original format and print the file in exactly the same way and with the same quality as its native program. Acrobat Reader™ can be downloaded at no cost from *http://www.adobe.com.* A full version of Acrobat™ used to create files, can be purchased from Adobe. Other products are available for displaying file formats, but at the time of release of this publication, Acrobat™ is the industry standard.

E-mail Software

Communication by e-mail was one of the first uses of the Internet and continues to be the most popular use today. Browser-based web services available through subscription, often at no cost, enable people to access their e-mail from any computer with an Internet connection. Many people prefer to use an e-mail client, a program devoted exclusively to sending and receiving e-mail messages and graphics. Some of these programs are loaded on new computers or are available through other means at little or no cost to the user.

Browser based e-mail services often contain advertising in the form of "spam," the electronic equivalent of unsolicited junk mail. Spam received through many web-based e-mail programs may not be filterable, since the subscriber agrees to receive these messages when accepting the conditions of service. Another hazard of spam is that it can serve as a vehicle for viruses. E-mail issues, such as whether to permit use of web-based e-mail providers, should be addressed in the agency's Acceptable Use Policy (AUP).

The dedicated commercial e-mail programs are usually more sophisticated and offer greater protection for the user. One of the tasks of the needs assessment process is to determine what kind of e-mail software will be most effective for the agency.

Virus Protection Software

The use of virus protection software is crucial for all Internet users and users of shared files. These programs often come with new computers, but if not, a virus protection program should be purchased separately. As new viruses emerge almost daily, the program should be updated frequently to protect the user and other users who may be connected through a network or included in a list of contacts.

Virus protection software can be purchased for individual computers or licensed for use by all agency computers. This software can also reside on a server, with users able to update the software on their desktop computer over the agency network.

Web Development Software

For agencies planning to launch their own web sites, a means of creating web-compatible files is essential. Historically, programmers wrote original source code to create most web files. Today, many word processors and some office applications and browsers include programs that will automatically generate the code needed to display documents on the web (e.g., HomeSite™, Front Page™, Dream Weaver™, etc.).

More sophisticated software applications that are designed solely for the creation and management of web sites are also available. Among other functions, these programs can create a map of the web site and its links, permit the user to split graphic files for creation of special effects, split web pages into separate panes that permit the display of multiple files on a single screen, and automatically generate code for a multitude of other formatting options.

File Transfer Protocol Software

Internet files are written on a local computer and are then transferred to an Internet server where they are made accessible on the web. Programs that permit the easy transfer of files between local and remote computers without opening and viewing them in a browser are known as file transfer protocol or FTP clients. FTP software enables a remote user to control functions for moving, saving and deleting files over the Internet or other Internet Protocol (IP)-based networks. Some web editors include publishing functions that permit the user to save his or her files at the remote location; FTP software includes features that provide more flexibility and often greater speed for the transfer of files, including files that cannot be handled by the web editors.

Mailing Lists and Subscription Lists

Mailing list software and subscription lists are valuable communication tools, but they have an etiquette all their own and can be a source of misunderstanding and frustration if users are not aware of the potential pitfalls. For example, a frequent source of aggravation is the general posting of subscription cancellations to an unmoderated list. Users should know that there are at least two separate addresses for mailing lists. One is the posting address to which all replies and new messages are posted and from which all messages are forwarded to subscribers. The second address is for the server site where cancellations or requests to change parameters of the subscription are sent. Messages posted to the server address are not seen by other subscribers and do not interfere with discussion topics. Most lists greet new users with a welcome message that tells them how to access various services available through the site.

An effective mailing list server host should send an initial welcome with a description of the procedures and addresses used for public and nonpublic communication through the list server. In addition, it should periodically send out a review of the procedures and etiquette for the site. Responsible subscribers should save the welcome file in a location where they can find it later in case they wish to cancel their subscription or change the way they receive messages.

Bulletin Boards

A bulletin board permits the posting of information to a site that can be accessed remotely by subscribers or others with access to the site's address or Uniform Resource Locator (URL). Mailing list software automatically sends new postings to all subscribers,

one message at a time or in a digest format sent at specified intervals. The advantage of mailing lists is that new postings are delivered directly to the subscriber instead of the subscriber having to actively seek them out. Subscribers may be permitted to post messages to both *moderated* and *unmoderated* mailing lists. Messages sent to an unmoderated mailing list are posted automatically, while those sent to a moderated site are posted and distributed after review by a human moderator.

Software for a More Useful Server

If the agency plans to host its web site on its own server, it will need software to control the server functions. A resource to assist the agency in reviewing and evaluating server software is available at *http://serverwatch.internet.com*. The capabilities of Internet-based software continue to progress in step with user sophistication and increasing web site complexity. A few examples of the web site tools available to educators today include software that:

- tracks access to individual files within a web site;

- permits remote access to databases for viewing and downloading data in a format that can be analyzed and manipulated;

- assists school organizations in creating and delivering instructional content via the Internet;

- tracks the use of curriculum standards; and

- enhances the actual delivery of instruction within schools and classrooms.

Agency web sites can be as simple as displaying aggregated data in report format for viewing only or as complex as making data available to users for download and analysis. The latter requires a database that is configured for web connection and typically requires special training of personnel managing the database.

Just by having a web site, many avenues to enhance the delivery of the instructional program will be available to the agency. From expanded resources to programs that simulate historical events to self-paced courses, the web can open up a whole new world for students and teachers.

For an education agency with unique needs that cannot be met adequately by commercial software, customized software written by a professional programmer may be a sensible option. This is true when considering administrative or instructional programs.

Purchasing Hardware to Host a World Wide Web Site

The minimum hardware needed to host a web site, list server, or other Internet service is reasonably obtainable. The server should have a relatively high-speed processor and a great deal of Random Access Memory (RAM) with any reliable operating system. Web server software is necessary, along with a properly configured router that includes network and security software, for safe remote access to the server. The server should be connected to the Internet through a high-speed portal with an ISP. The connection must include a static IP address and a domain name registered with an Internet registrar, such as InterNIC, Network Solutions, or, register.com.

The hardware needs assessment enables the agency to determine the complexity of the site.

This minimum configuration will support a small web site with relatively little traffic. As the web site, mail server, list server, or other Internet traffic increases, and as the site itself becomes more complex, the agency will need to consider integrating more advanced equipment into the site. This equipment might include a higher speed processor, multiple processors, more storage space, or a connection with greater bandwidth and more access portals.

A crucial component in the purchase of equipment and software, as well as in the operation of the server, is the participation of a technician who has the formal training and knowledge to maintain a reliable system. Smaller agencies sometimes rely on a knowledgeable teacher or staff member, or even a student, for technology guidance. This approach may be initially successful, but as the web site becomes more sophisticated and, particularly, as the system becomes accessible to the outside world, it becomes imperative that a system administrator with extensive technical training be available to maintain confidentiality of student and staff information, as well as security for the agency's equipment and users.

At a minimum, a person with reliable technical knowledge, as well as a person familiar with an understanding of the legal issues surrounding purchasing and procurement, should review the agency's RFPs and bid specifications before they are published. The more planning and detail involved in the RFP specifications, the more likely the agency is to obtain a quality product at a reasonable price.

Purchasing the necessary hardware is but one essential step. In appendix C information is provided on how to connect this hardware to the Internet.

Summary

An education agency must consider a number of essential issues before deciding whether to develop and maintain a web site in house. Most critical is the availability of a qualified staff of sufficient size and expertise to carry out all aspects of the Internet implementation effectively. If agency resources are insufficient, it may be preferable to outsource all or part of the operation. Regardless of the outsourcing decision, continual professional development is essential for effective use of the Internet. Issues to be considered in outsourcing decisions include the following:

- Matching expectations to the agency's capacity. A well-designed web site with static pages containing valuable information is more useful than an interactive site that is out of date or unreliable.

- Technical staff with the expertise to maintain a reliable and secure system.

- The resources to obtain a server, server software, and security software for agencies wanting to launch sites that are more sophisticated or host their own web services.

- If required, specialized software for list servers, bulletin boards, databases, or other services.

- The ability to upgrade equipment and expand bandwidth as sophistication and use of the site increases.

Procuring Resources

Introduction

In the 1990s, with the spiraling popularity of the Internet, education communities were eager to bring Internet access to the classroom and to build a presence on the web. A rush to purchase hardware and software often led to mistakes in technology choices. Since then, many school districts and state departments of education have developed a more systematic approach to technology procurement. This chapter describes procedures to make sure that technology purchases, especially for web site development, meet the needs of the agency.

In some agencies, a funding request with supporting justification is needed for every technology purchase. With solid planning, technology development and systems upgrades could become a permanent line item in the annual budget. It is more efficient when a line item for technology is included in the agency's budget. As educators develop plans to meet technology needs, policymakers should be prepared to provide a reliable funding source.

Under the best circumstances, a technology plan will guide all technology-related purchases. However, no plan can anticipate every need, so it is essential that technology budgets include some contingency funds for unanticipated purchases related to emergencies and changing technologies. In addition to emergencies, agencies need to budget for planned maintenance and upgrade of both hardware and software. For a reliable and useful network, policymakers responsible for approving the agency's budget and purchases should have a clear understanding of the total cost of ownership. Costs beyond the initial purchase cannot be an afterthought.

QUESTIONS ANSWERED IN THIS CHAPTER:
- **What is a bid process?**
- **What are the components of a bid request for building a web site?**

> **Technology should be an integral part of an agency's budget.**

The Bid Process

Some people may view a public bidding process as inefficient, time-consuming, and restrictive. However, there are several reasons why such a process should be employed in technology purchases.

- Because bidders are unaware of the price being offered by their competitors, the possibility of lower initial and continuing costs is more likely.

- A properly administered public bidding process eliminates the legitimacy of complaints from vendors and citizens that purchasing decisions were made through collusion and favoritism.
- The agency is able to request special combinations of products and individually designed services without having to pay for unwanted components that often come with package deals and off-the-shelf purchases.
- The process can provide an objective set of purchasing criteria that will assure that the purchase supports the mission and operational needs defined in the agency's strategic and technology plans.

Bid requests may fall into any of several categories. Technical specifications are most commonly used for the purchase of specific equipment. The specifications will set a minimum standard for components, service, warranty, and other agency needs. Well-written specifications can help in standardizing the components on a network and assuring compatibility of products. Good specifications can also provide strong evidence supporting the agency's position concerning the scope and intent of the parties when a dispute arises between the agency and a vendor.

Most often, specifications will designate minimum standards for functionality and quality. Typically, they do not designate a particular brand and/or model. In some cases, the minimum standards may be set by referring to a specific model and, by using the phrase "or equal," will permit vendors with alternative products to demonstrate that their proposal will result in functionality and quality equivalent to or better than the product specified.

> **RFQ = Request for Qualifications**
> **RFP = Request for Proposal**

A Request for Qualifications (RFQ) is often appropriate when the agency is purchasing services (which may include some equipment) and does not yet have a specific vision of project goals and desired services. The RFQ is used when seeking specialists to help define and, perhaps, manage a project. Because the successful vendor will be assisting the agency in defining the project, it often leaves the question of pricing open to negotiation.

A Request for Proposal (RFP) may be the preferred bid document for securing goods and services when the agency has already determined the purpose and scope of a project. The RFP asks vendors to describe, or propose, how they will assist the agency in achieving its stated goals and why that vendor can provide a better service than others. In most cases, the RFP will include pricing information and may incorporate qualifications and other components found in an RFQ.

Components of Bid Requests

A good bid request defines what the agency wants to purchase with enough specificity that the comparison of equipment, services, and prices among the proposals will provide a fair and objective basis for identifying the best value and for selecting the best vendor.

Many agencies use templates as starting points for developing their bid requests. These templates can save time and energy, since some parts of different requests will be the same. A template may exist, for example, for the information needed by the local newspapers for posting the legal notice. Additionally, templates can address local and other governmental regulations. Finally, when responses to bid requests are submitted in the same format, using a template supplied by the requesting agency, it may be easier for agencies to evaluate the proposals.

After writing a bid request, the agency may want to consult with a business administrator, legal counsel, or other qualified individuals to examine it and ensure proper compliance with district, local government, state, and/or federal regulations. Many agencies have procurement personnel or business officers who can lead staff through the purchasing maze and review that process with them.

Listed below are some aspects to consider in preparing a bid request for web development. The agency should also consider having a person knowledgeable about web site development from outside the agency review the request to ensure that it covers all of the agency's needs.

Legal counsel should review bid and proposal requests.

These guidelines are intended to provide a broad overview for preparing a variety of bid requests. Details of an actual request will depend upon the specific needs of the agency. The request process may also vary, not only according to specific types of purchases, but also according to state and local laws and policies. Education agencies should develop a consistent set of procedures, reviewed by legal counsel, to govern all bid and proposal requests.

Bid Request Components

Basic design parameters

✔ Determine how the development of the web site fits into the strategic plan of the agency.

✔ Define the fundamental message(s) to be communicated on the web site.

✔ Set forth the basic structure of the site, with a description of the component parts.

✔ Note that an effective needs assessment and technology plan will forestall multiple changes during the design and development phase, which will help control costs and speed the process for timely implementation.

Contract parameters

✔ Develop a *statement of work* that clearly defines the roles, responsibilities, deliverables, timelines, and costs.

✔ Define whether the scope of the contract will be for design and development only or will include vendor operation of the web site after deployment.

✔ Specify the level of support services needed after deployment—whether the vendor will manage the site or simply provide troubleshooting and repair.

✔ State the condition under which maintenance is required after the web site is developed and placed online.

✔ Establish a clear price structure (only in very limited circumstances should the contractor be allowed to price on a time and materials basis).

✔ Define a payment schedule.

   • Payment should be based on specific deliverables or benchmarks.

   • Deliverables can be written into the RFP, but may require some additional negotiation.

✔ Set reasonable timelines and benchmarks for development and completion.

✔ Ensure that the education agency will receive sufficient documentation to be able to use and maintain the site after deployment.

   • Determine how and when documentation will be delivered.

   • Determine the form of the documentation (e.g., written guide, online guide, etc.).

✔ If professional development is a component of the bid proposal, determine where and how the vendor has provided this service in the past.

Bid Request Components *(continued)*

Vendor/contractor qualifications

✔ Define the training and expertise necessary for vendor/contractor respondents in areas such as:

- graphic design skills;
- writing (i.e., composition) skills;
- knowledge of web programming languages; and
- experience with online course development.

✔ If the web site is to include a database, require that the vendor/contractor provide evidence of expertise with the programming of at least one large database (e.g., SQL, Oracle, Informix) and the web-based user interfaces for the databases.

✔ If necessary, specify a database to be used by the agency if the use of a database will involve interaction with other computer systems that are already in the agency.

✔ Require bidders to document expertise in web-programming languages (e.g., HTML, SML, ASP, VBScript, Java, Perl script).

✔ Require evidence of company stability (e.g., financial reports and history).

✔ Require access to other sites designed and/or operated by the vendor.

✔ Require the contractor to demonstrate knowledge of the web "Content Accessibility Guidelines" (see appendix F) and Section 508 of the Rehabilitation Act [29 U.S.C. 749d] standards.

✔ Require the contractor to document individual qualifications of the staff who will work on and be responsible for the agency's site.

✔ Require the contractor to present a proposal based on the agency's needs assessment and technology plan.

✔ If the web site is to be housed outside the agency, include a provision that allows for upgrades of server speed and bandwidth.

Legal issues

✔ Establish ownership of source code or the computer program(s) used to create the web site. The ownership of source code is critical because the agency may later decide to change vendors or bring maintenance of the site in house.

✔ For any development supported partially or completely by federal funds, the code automatically becomes part of the public domain. Inform vendors of this stipulation up front to avoid misunderstandings and/or future legal conflicts.

✔ If the web site is to be housed on servers outside the organization, establish that the web site is owned by the agency and may be moved to a different vendor, or brought in house at a predetermined time.

✔ Ensure compliance with copyright laws and provide indemnification for the education agency for any copyright violations made by the vendor.

Summary

The process of developing a web site progresses through technology planning, assessing specific needs, and the gathering of funding sources. When the agency is ready to develop a web site, a formal bid process has many benefits. An RFQ or RFP allows vendors to respond to the specific, stated needs of the agency.

- Funding for technology, including web development and support, should be built into agency budgets.

- The bid proposal for web development could include the following areas:

  - basic design parameters;

  - contract parameters;

  - vendor/contractor qualifications; and

  - legal issues.

- Legal counsel should review the general procurement procedures for the agency for compliance with legal and generally accepted accounting principles.
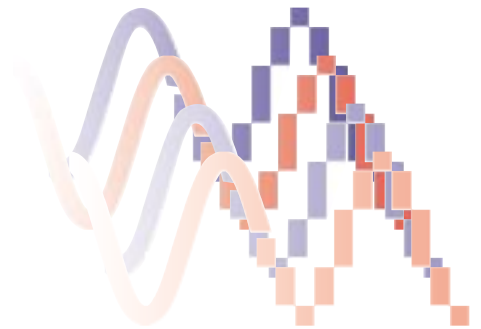
Maintaining a Secure Environment

Introduction

Security is a process that focuses on "CIA": confidentiality, integrity, and availability.

Education agencies thrust into the world of computer networks and electronic communications are often unprepared for the related security risks and are unaware of many of the strategies that can protect their system. The agency's technology officers or technical staff working directly with Internet or intranet (i.e., internal networks, as opposed to the outside world of the Internet) networks will most readily appreciate the technical aspects of security presented in this chapter. Nontechnical staff should find the broader discussion of security helpful in understanding the absolute necessity for and value of securing all facets of the agency's network.

The recommendations in this chapter are detailed and extensive. Education agencies must be prepared for every eventuality ranging from a careless employee walking away from a computer station that is logged onto a sensitive data site to a hacker trying to break into the agency's system to physical destruction of the network by a tornado, hurricane, or earthquake. An agency involved in maintaining a computer network, especially one with Internet access, should use the information in this chapter to identify and resolve system vulnerabilities and in so doing reduce the risk of liability.

The security recommendations described in the chapter are solid, fundamental business practices that are, for the most part, not unique to the education sector. However, because education agencies are responsible for ensuring the physical safety of children in a stable environment that fosters learning, the obligation to extend security precautions to online computer information systems is especially strong. In addition to student safety, other areas at potential risk include the confidentiality of student, staff, or financial data sent or received through the Internet; the integrity of intellectual property; and the investment in hardware, software, and other resources.

When considering security precautions, education agencies in particular should take note that the greatest exposure to risk comes from within the organization. Internal agency employees perpetrate most network security violations. Malicious, or even unintentional, corruption of data, hardware, or software can be crippling to any enterprise. Illegal acquisition and disclosure of sensitive student information can harm a child and ultimately the school system.

> **An agency should assess the legal and financial ramifications of failing to make a reasonable effort to secure the network and its many components.**

The following key areas for strategic planning organize the discussion of network security in this chapter. The following methods for securing each component of the network, whether a local or wide area network, are presented:

- security assessment;
- securing hardware;
- securing operating systems;
- securing software (applications);
- securing the network, including wireless networks; and
- data security.

Security Assessment

The first question to ask is what needs to be done to provide appropriate security for the agency's network? The total network is only as secure as its weakest link, and, as mentioned, most security breaches occur from people who work inside the agency itself. For this reason, the implementation of very simple security measures, many of which are free or are inexpensive, can provide significant protection for the total network.

The first step is to perform a security assessment. If multiple agencies are connected to a larger intranet (a private network that provides users access within the agency and to the public Internet), the security assessment is ideally performed collaboratively. Common security strategies should be employed throughout this intranet and for all components of the network.

In performing a security assessment, the agency should address each of the topics discussed in this chapter. In assessing the level of security, agency staff should

- identify each point of potential failure in the system and assess how each failure would affect the agency;
- prioritize the points at greatest risk or those that would cause the biggest problems for the agency; and
- ascertain one or more solutions to secure those points and determine the costs associated with each solution.

A security plan should be written under the auspices of the district technology director, but should involve other agency representatives. When developing the plan, the agency should consider the following issues:

- The plan should be drafted for adoption by the governing body.
- The plan should take into consideration the information gained during the assessment phase.
- System users should be educated about the plan and its importance to the agency.
- System users should be consistently informed of changes to security procedures.
- The agency should regularly appraise security protocol and should revise or update the plan as needed.

Securing Hardware

Hardware security includes the physical protection of equipment (e.g., computers, printers, monitors, etc.) from both theft and damage. Different types of hardware require different types of protection. Servers and related equipment should be placed in a secure room with limited access. The room should have proper environmental conditioning and fire protection equipment.* (i.e., fire extinguishing systems should be used in areas where water cannot be used).

While this may seem obvious, an asset (inventory) control system will assist with the agency's technology planning efforts. Without an asset control system, the agency will be unable to determine what hardware exists or where it is. This system is also important so that the agency can determine which computers, or other systems, need to be replaced as they become obsolete.

Along with the obvious fact that proper security deters theft of property, effective hardware security bars unauthorized access to the server. Proper security prevents people from tampering with server settings, corrupting data, or gaining access to unauthorized programs and confidential information. Measures for securing hardware systems include the following:

- allocate dedicated building space to house centralized hardware;
- maintain controlled entry (e.g., card, key, combination lock access);
- make certain that a proper fire protection system exists;
- maintain proper temperature and humidity controls;
- evaluate the need for adequate electrical power, including power for air conditioning;
- provide emergency sources of power (e.g., UPS battery backup, alternative electrical generator);
- arrange equipment placement within equipment racks and on the floor in a way that allows adequate ventilation;
- monitor the room environment and electrical systems; and
- use network monitoring and *packet-sniffing* (see below) utilities that display and log data traffic to detect the installation of unauthorized hardware and/or software applications (i.e., monitor for protocol violations, bandwidth-intensive applications, etc.).

Securing Operating Systems

The operating system (OS) is the underlying computer system on which application programs run. Choosing an OS is a critical decision that directly affects the security measures an agency must take. Some OSs are easy to use but less secure. Others are more complicated to maintain but when properly configured are virtually impenetrable. Whatever the choice, the system must be "hardened," or secured, by removing unneeded functions, restricting access, and tracking changes and processes.

If, for example, a port (i.e., a doorway into a system) is left open unintentionally, it can become the door through which an intruder can enter the network. Conversely, if the system is secure, intruders will have a much more difficult time entering the system.

Many OS options are available, from "UNIX-like" freeware (public domain software offered at no cost) to various Microsoft and Apple products, which vary in acquisition

---

* Halon gas is believed to deplete the ozone and is no longer produced in the United States. Use of Halon has not been banned, and may still be available, but the U.S. Government recommends alternative methods.

and maintenance costs. Acquisition cost does not necessarily indicate the power of any particular OS. The agency should ensure that the hardware and OS combination is robust enough for the intended purpose. The OS must have the ability to be configured to meet both the service *and* security requirements of the agency.

The criteria for the OS selection should be based on the agency's needs assessment. The agency should take into account the resources necessary to support the OS. If the agency chooses to run a *mixed environment* (a combination of hardware and software utilizing more than one OS), it should be sure the support resources required to maintain this configuration are available. A mixed computing environment requires additional expertise and resources in order to maintain proper security.

OS security consists of limiting access to network resources, such as centralized applications, files and directories, network printers, and other such components. Personnel should have network access only for the specific tasks related to their work. An appropriate policy for OS security is a baseline denial of access to all components by all personnel, with explicit access privileges granted on a case-by-case basis. User login credentials identifying the role(s) and profile of the user should "describe" the user's access parameters to the OS. The extent of access to network resources granted to the user should be based on the individual's authorized role/profile.

Different operating systems regulate user access in different ways; however, each provides similar functionality by assigning Read, Write, and Execute permissions on directories, files, network printers, etc., to groups of users or individual users as required. Some access-related security measures that should be implemented are as follows:

- disable guest accounts;
- change default passwords;
- force frequent user password changes;
- allow only nondictionary passwords, that is, a combination of alpha and numeric characters;
- deny access by default;
- restrict off-hour access unless the user requires 24/7 access;
- for ease of administration, control access based on groups, profiles, and policies;
- assign users into the smallest possible groups to eliminate unneeded access;
- designate a system administrator backup to adequately cover leave times;
- require administrator access through a different login mechanism, *not* through the normal user login;
- allow only needed services to run on the network (e.g., Telnet, web, RSH, FTP, NTP, etc.);
- allow only authorized administrators to install software;
- allow only needed protocols to run on the network (e.g., IPX/SPX, Appletalk, NetBEUI, TCP/IP, DLC, SNMP, etc.);
- integrate TACACS+ or RADIUS authentication into the agency's firewall to avoid unauthorized Internet access; and
- enable firewall, virus, intruder detection, and network monitoring software (see below).

Securing Software (Applications)

As noted earlier, software programs are applications that run "on top" of the operating system. The most common applications are information systems, word processors, spreadsheets, e-mail programs, and web browsers. There are literally thousands of

applications available. The purpose of this section is to provide education agencies with recommendations for securing software applications. Security in this area will limit (not eliminate) copyright infringements, assist in the proper licensing of software, and attempt to ensure that only authorized persons have access to software installation media.

Software installation media should be stored in a centralized location with proper documentation of the number of licenses and number of installations. These media should be protected from harsh environmental conditions, such as excessive heat, moisture, and electrical and magnetic fields (EMF).

All software media should be backed up regularly to ensure that no data are lost. Periodic backups stored in a secure off-site location will make it possible to recover quickly from a catastrophe on site. The agency should take into account regional peculiarities when storing backups off site. For example, in areas prone to earthquakes, media should not be stored in high-rise buildings; in areas prone to flooding, media should be stored in a facility away from the flood plain.

Some recommendations for software security are as follows:

- store software media in a locked cabinet within a proper environment;

- retain off-site storage for backups of installation media;

- test the process for restoring software;

- retain off-site storage of licensing and application documentation;

- maintain and back up licensing management and related documentation;

- allow access to applications through the use of network security settings to only those groups/users that require access;

- implement a software-auditing package to ensure license compliance and to ensure that no unauthorized software has been installed on the agency's system;

- standardize applications across the agency;

- use virus-scanning software with frequent definition updates (network-attached appliances are available for e-mail virus scanning); and

- use spamming prevention or filtering software to prevent unauthorized entry of e-mail (e.g., do not allow web-based e-mail programs, such as Hotmail™). Unauthorized e-mail entry is a serious vulnerability that can lead to the entry of viruses into the network through a "back door."

Securing the Network

The same security procedures in place for server hardware apply to equipment that supports the network, including switches, hubs, routers, firewalls, access points, cabling, etc. Network equipment should be installed in an environment with proper ventilation and power requirements and should be protected from unauthorized access. The agency should place the equipment in dedicated building spaces. Access should be limited to staff that have a key, combination lock, key card, or other security device. Some basic precautions for securing network equipment are as follows:

- limit access to network equipment to authorized individuals;

- do not allow users to install unauthorized network equipment;

- use secure, encrypted passwords for "root" access (access to the "root" enables users to control entire systems or servers); and

- ensure proper cabling and cable protection by
    - running cabling under a false floor,
    - avoiding running cable over fluorescent lighting fixtures, and
    - staying within cable/fiber length requirements.

A fundamental action the agency can take toward maintaining a secure and reliable network is to hire a qualified individual to serve as the network administrator. Network administration is not a task for the average high school teacher/technology coordinator. Many agencies, however, cannot afford to hire an experienced network administrator for each school and often do rely on faculty for this position. If a teacher/coordinator is to be responsible for a school network, the agency must recognize training and professional development as priorities.

Agency network policies and procedures should be clearly defined. These policies should be made readily available to anyone responsible for maintaining the network. Listed below are some items to consider for agencies managing their own networks. The responsibilities of a network administrator are, for the most part, very technical in nature. This reinforces the point that training is critical for anyone with the responsibility of running a network. Agencies should

- assign one individual to be responsible for network administration (and one individual as his/her backup);
- limit access to network equipment console screens by login credentials (either on the piece of network equipment or using an authentication server);
- limit access to Telnet sessions on network equipment through access lists and/or authorized workstations where only authorized users have access;
- limit protocols running on the network equipment;
- configure login banners to warn intruders of possible prosecution;
- use firewalls to prevent unauthorized access between external and internal systems;
- use unroutable IP addressing schemes within the internal network
  [Class A – 10.0.0.0-10.255.255.255 (10/8 prefix),
  Class B – 172.16.0.0-172.31.255.255 (172.16/12 prefix),
  Class C – 192.168.0.0-192.168.255.255 (192.168/16 prefix)];
- utilize intrusion detection systems (IDS);
- inspect, analyze, and maintain router audit logs;
- provide ingress and egress access control list (ACL) filtering to prevent IP spoofing; and
- eliminate unauthorized network resource use by
  - monitoring network traffic and bandwidth usage and protocols to ensure adequate bandwidth for applications;
  - removing the ability to download unauthorized files;
  - restricting remote access to network resources to authorized individuals with types of remote access including dial-up connections, virtual private networks (VPN), and Point-to-Point Protocol (PPP);
  - implementing a multiple-authentication policy for authorized users or integrating into an authentication server;
  - eliminating any "back-door" types of equipment (e.g., user modems installed on desktops);
  - maintaining proper encryption of remote connections to ensure confidentiality; and
  - using VPN technology with proper encryption to gain connectivity through the public networks such as the Internet.

See page 37 for a depiction of a sample, secure network.

Securing a Network

Internet

Routable IP Addressing

Border Router

Edge Router

Outside Switch

Redundant Failover

RFC 1918 IP Addressing

Firewall

DMZ LAN (or VLAN)

NOTE: Must be hardened against attack and only accessible to Administrative Hosts

IDS Host

CFS Host

INSIDE LAN

Admin. VLAN

OME VLAN

Inside Switch (or VLAN)

Router to Other Facilities

Server (4) (Admin. Syst.)
- Tacacs+
- Radius
- Enterprise Systems
- Data
- Printing, etc.

Network Monitoring Station/Tools
- Log
- SNMP

Administrative Hosts

Mail Server

Web Server

Network Monitoring Station/Tools

Non-Administrative (Student) Hosts

CFS Host (Interacting w/Firewall)

By: Joe Pangborn, Director of Information Technology, Roger Williams University

Wireless Networks

Wireless communication is a rapidly evolving technology that is becoming increasingly prevalent in everyday life. The built-in security for wireless computer networks, however, is relatively weak. Technology coordinators need to pay particular attention to secure these networks properly, and the network administrator must keep up to date on emerging methods for securing wireless networks. Some security measures to consider when planning a wireless network are as follows:

- shut off Service Set Identifier (SSID) broadcasting and use an SSID that does not identify the agency by name;

- select a hardware vendor and software revision that has fixed the problem of randomization of initialization vectors (IVs);

- utilize applications like AirSnort or BSD-AirTools, which will be less likely to crack the agency's Wired Equivalent Privacy (WEP) keys;

- use 128-bit WEP and change WEP keys regularly. Select a vendor that provides a tool to rotate the agency's WEP keys;

- disallow access to resources at the first router hop other than the agency's VPN server, which ensures that the only host available to the wireless segment is the VPN server until a tunnel is established;

- place wireless access points on a dedicated virtual local area network (VLAN). Do *not* mix wired and wireless clients on the same LAN segment;

- implement a policy that limits the amount of connectivity a wireless client has to the agency's network. Assess whether students/faculty/staff need more access than TCP/80, TCP/443, etc.;

- utilize personal firewalls on the agency's workstations; and

- disable automatic IP address assignment (DCHP).

If hackers are able to guess or crack the agency's WEP keys, they will not be able to access the remainder of the internal network because VPN and VLAN architecture with access lists will allow only authorized VPN clients to be routed to the network from a wireless VLAN segment. Hackers will be able to attack clients on the same subnet, however, and if one VPN connection is left up, it could be abused to access the rest of the internal network**.**

Network Reliability

Reliability of the network is a key to daily business operations and to an effective instructional program. Everyone in the school hears about the times a teacher has scheduled a web-dependent lesson only to be unable to access the network. It is imperative that "mission-critical" applications (e.g., financial systems, student information systems) always be available to those who depend on the systems.

Network architecture designed for redundancy, with built-in backups for primary resources, minimizes the incidence of network downtime. When considering this issue, the agency should take into account the extent of redundancy needed.

Where it is possible, consider redundancy in both LAN and wide area network (WAN) architectures during the design phase. The agency should select redundant service providers that use separate infrastructures. Some specific redundancies that can be built into the network apply to

- the local loop for WAN connectivity;

- switch management modules with redundant connections;

- power sources for network equipment backed up by monitored UPS systems;

- power supplies in network equipment;
- network management (supervisor) modules in network equipment;
- cabling, as required; and
- redundant cabling in redundant conduits, ducts, or poles. Having a second cable running through the same conduit as the first provides little protection. For example, a conduit could be dug up by an "uncaring" backhoe destroying both primary and redundant cables.

Another measure to maximize network reliability is the implementation of intrusion detection systems. Intrusion detection systems are host-based or network-based software that monitors attempts to break into and gain access to the network. These systems watch data packets as they transit the network outside the firewall. They monitor attempted port scans, distributed denial of service (DoS) attacks, and other intrusion attempts. Intrusion detection protocol should include the following tasks:

- install and configure an intrusion detection system;
- enable port monitoring outside the agency's firewall;
- review intrusion detection system log files daily;
- configure blocking on the router (e.g., "black hole routing" of unwanted data) to head off severe hacking attempts; and
- contact the organization that owns the address of the attacking IP address. Tools such as nslookup, tracerroute,or the following web sites can help identify the owners of the IP address space from which an attack originated:
    - *http://www.arin.net*
    - *http://www.netsol.com/cgi-bin/whois/whois*
    - *http://www.internic.org/whois.html*

Data Security

Data drive the engine of each educational organization. From payroll records to "data-driven decisions" about instructional programs to student information systems, human resources files, transportation information, and student portfolios—data integrity is critical.

Keeping data secure is the primary mission of those in charge of technology. Protecting the agency's data by implementing robust architectures and comprehensive backup and recovery plans is extremely important. The agency must take every precaution to prevent unauthorized users from changing data, deliberately or inadvertently, by way of a "hole" in security procedures. Security holes can occur from outside through the web or internally from within the LAN.

The following recommendations for maintaining data security are based on using Redundant Array of Independent Disks (RAID). This allows the same data to be stored in different places on multiple hard drives. When using RAID, the following steps should be taken:

- Data files should be stored on separate logical drives consisting of a RAID-5 (stripped set) array of physical devices.
- Transaction logs should be stored on, at least, a RAID-1 array (mirrored).
- Applications should be installed on either a mirror set (RAID-1) or stripped set (RAID-5) and should be backed up when installed, changed, or updated.
- Operating systems (OS) should be installed on, at least, a RAID-1 array and be backed up when they are changed.

- OS, applications, and data should be stored on separate physical and logical drives (e.g., mirror set 0 to contain the system, mirror or stripped set 1 to contain applications, stripped set 2 to contain data).

- Consistent backups of data off site should be maintained.

- Robust network-attached storage (RAID-5) or storage area networks to maintain online or backup data should be used.

- Clustered server architecture should be considered if the information stored is "mission critical."

Backing up Data

The reasons for backing up data are obvious. However, many agencies (both inside and outside the education community) do not take this task seriously until they lose data. When the payroll information cannot be found or when all the student information entered into the system during the day is lost, people will pay attention to backing up data. It is better to pay attention before a disaster strikes.

For years, personal computer users have been told to back up their data files. With a personal computer, backing up data and storing the backed-up data are relatively simple processes—that is, when people remember to do it. The potential consequences for failing to back up education agency data are magnified when dealing with a network of multiple users and applications that could affect the lives of those users.

A comprehensive procedure for backing up agency data is imperative. Of equal importance, staff must follow the procedure. When designing its disaster recovery plan, the agency should consider the frequency of backups (e.g., full, incremental), as well as available hardware, the system configuration, and the amount of data (and its importance) to be backed up.

Agencies located in areas where there might be earthquakes, hurricanes, or other natural disasters will understand the need for developing a backup procedure that uses removable media that can be transported off site. All agencies are vulnerable to some type of disaster. The solution is to have a backup plan and an off-site storage facility. Any of the following media are appropriate to use for archiving data:

- removable storage,

- magnetic tapes,

- CD or DVD devices, or

- network-attached storage.

Some backed-up data should be available at all times. For example, while it may be critical to have payroll system backups available on hand, the same degree of urgency may not apply to student portfolio information. Creating a clustered server (i.e., a group of servers clustered together and used to back up the data in various ways) environment increases the likelihood that necessary data will be available when they are needed. The following architecture options are available for clustered environments:

- *Load-balancing* environments are clusters of servers arranged to share the load of user requests. Web servers typically use this environment.

- *Hot standby* environments require an identical server attached directly to the primary network server (for monitoring) to immediately take over filling user requests in the event of a primary server failure.

- *Cold-standby* environments also consist of a secondary server to which data are frequently updated. In this case, the secondary server must be manually put into operation upon a failure of the primary server. One advantage of this option is that it removes the need to maintain identical servers with interlocking hardware.

A backup procedure will not work if no one follows the procedures.

Documentation

Documentation of data file structure, metadata, and system architecture design criteria is essential in any data security plan. In the event of a nonrecoverable failure, the need to recreate an identical architecture is much easier with proper documentation. In the world of technology, with staff moving from job to job, having proper documentation will help new employees. They will be able to provide appropriate maintenance much more quickly if they can refer to written documentation.

Often documentation is provided when a network is first installed. It is up to the agency to allocate time so the technology personnel can update the documentation. Otherwise, the old documentation may be of little value.

Documentation = Protection
Out-of-date documentation = Very little protection

Data Integrity

Data integrity is vital for any organization. Having poor data is worse than having no data. Maintaining proper data constraints, validation rules, and application controls, such as those identified below, can help to ensure that data correctly input into the system remain intact:

- No person, other than the database administrator (DBA), should have direct access to data for input or change. Other staff should use applications or programs designed for data input and update. These programs usually have "edits" and other programmed devices to ensure that data are entered correctly. When data are input or changed directly in the database, this protection does not exist.

- Data applications must contain validation rules, format masks, and data-checking algorithms to ensure data integrity prior to committing to the database.

- Online applications must contain the same rules as data applications.

- Database servers should reside on a secure segment of the network (i.e., behind or inside the firewall).

- Applications should be constructed to a three-tier environment (i.e., database server, application server, and client).

- Security should be set so that the user logs into the application server (*not* the database), with the application server having credentials to go to the database.

- Proper database design and implementation are essential for maintaining data integrity. Considerations should include archive log rollback segments and rollback log files.

Database Security

Database security employs similar security measures as those for operating systems. Database security, like OS security, utilizes logons and passwords to authenticate users. Users are assigned to certain types of groups, which in a database environment are called *roles*. Systems administrators, backup operators, and standard users are examples of roles that can be integrated into the OS, so that, for example, OS administrators are automatically assigned to the systems administrator role of the database system. Database security can be maintained discretely or can be integrated with OS security. The advantage to integration is that the user requires only one logon for both systems.

Security measures implemented at the database system level are only truly effective if used in conjunction with proper security mechanisms implemented at the front-end application, such as dynamic web pages. Additionally, database design must include some security auditing measures, such as those that track when and by whom a particular data element was entered or updated.

As described in the above section on OS security, database security should grant user access to data resources, as grouped by role and profile, based on the respective functions. This profile grouping process is preferable to a method that merely grants access to individual users. As with OS security, the default database access security setting should be to deny access.

Transmission of data should be secured using protocol applications such as secure sockets layer (SSL) or secure shell (SSH), as described in the "Data Exchanges" section below.

Virus Protection

Staff training regarding virus protection is critical.

Software programs are sets of instructions written in various programming languages. These instructions are compiled or translated into binary numbers that enable a computer's central processing unit to interpret and implement actions. Computer viruses are specific types of programs designed to cause damage to a computer system's data.

Virus programs work in different ways and enter the computer via different methods. For example, a virus can be sent as an e-mail attachment, a macro (or mini-program) within a document, an executable program on a floppy disk, or by other means.

Virus protection software is an important component of a security system.

Virus protection software is a necessary system component that minimizes the possibility of data corruption due to a malicious virus by detecting and removing virus programs. Virus protection software can be purchased for individual computers, but it is most cost effective in large organizations to purchase a multi-user site license (an enterprise license) for the software.

Once installed, virus protection software must be updated frequently. People are creating new, and more destructive, viruses all the time. It is vitally important to download and install the latest updates as soon as they are available to ensure adequate protection of computer data.

Data Exchanges With Agencies Inside and Outside the K–12 Community

Education agencies have always exchanged data. Schools routinely send student transcripts to each other, and districts send transcripts to colleges and universities. The agency sending data must ensure that any transfer of student information meets the federal, state, and local regulations enacted to protect the privacy of students.

The Family Education Rights and Privacy Act (FERPA) provides guidelines for the protection of student privacy.

Current standard protocols in electronic data exchange use Electronic Data Interchange (EDI) and Extensible Markup Language (XML) formats. Both are standard electronic record formats that have been approved or are being developed to take advantage of protocols used by businesses and education agencies.

The design of data exchange formats must be carefully considered. Electronic exchange of confidential data, such as individual student records, requires the use of secure communications methods such as data encryption, virtual private networks (VPNs), or leased lines. Hardware-based encryption can be integrated into firewalls to create VPN tunnels over the public WAN. The movement of any private data over the public network

requires at least 128-bit encryption. Examples of encryption algorithms include DSA, RSA, 3DES, IDEA, etc. Internet Protocol Security (IPSec) is an industry-defined set of standards that verifies, authenticates, and optionally encrypts data at the IP packet level. Secure sockets layer (SSL) can use various ciphers, including RSA, DES, 3DES, MD5, RC4, etc.

Encryption of Data

RSA public key cryptography, named for inventors Rivest, Shamir, and Adleman, is widely used for authentication and encryption of data. The agency can apply for a Digital Signature Standard (DSS), a digital signature for the authentication of electronic documents, or a general digital certificate through a Certificate Authority web site such as VeriSign®. This can be accomplished by submitting information about the agency and its web server via an encrypted Certificate Signing Request (CSR).

Once the Certificate Authority confirms that the agency is legitimate, it uses the CSR file to generate and validate certificates for the applying agency. The Certificate Authority will then issue the agency a server certificate to be installed on the agency's web server.

People who want to access this secure web server must have the Certificate Authority's root certificate installed on their own browser (VeriSign® is preinstalled on most browsers). Then secure information can be exchanged.

Digital certificates are used by the SSL security protocol to encrypt, decrypt, and authenticate data. The certificate contains the owner's company name and other specific information that allows recipients of the certificate to identify the certificate's owner. The certificate also contains a public key used to encrypt the message being transported across the Internet.

For each user's SSL secured session with the secure server, the user's root certificate creates a unique public key for the browser to encrypt and decrypt messages sent to and from the server. Public keys are discarded once the transaction's session ends. Messages sent from and received by the secure server are encrypted and decrypted using the server's private key.

A public (or shared) key algorithm can be easily utilized to encrypt data files for exchange. This method requires the use of a software package, such as Pretty Good Privacy (PGP), to generate an encryption key pair. The private key is kept within the agency; the other key is given to the party to be granted access. Whenever a key is "compromised" or needs to be changed, the software can create new keys.

Digital Signatures

Digital signatures are digital codes attached to transmitted data that uniquely identify the sender. Digital signatures can be integrated into web applications to ensure that only properly authorized users are inserting or changing data in the application (and subsequently the database). Digital signatures are also used to identify the sender in secure e-mail transmission.

A digital signature consists of a private key and a certificate. The private key is a large number that exists on a user's computer. By using this private key, the computer generates a digital signature that seals a message with information (a series of numbers or a code), affirming the identity of the sender of the message.

In turn, a certificate contains a public key and identification data about the person who holds the private key. Certificates are freely distributed and are used to verify that a digital signature was valid and generated by the person who physically possesses the private key.

Where Are the Security Risks Coming From?

Throughout this chapter, various protocols and policies have been discussed for protecting individuals, data, and hardware. It is ironic that the greatest security risks come from the people these policies are designed to protect.

The leading security concerns for an education agency come from inside the network—teachers, students, or other staff who engage in unauthorized behavior, either knowingly or inadvertently. These activities may range from administrative staff taping the system password to the desk to a high school student showing off his/her hacking abilities to a student trying to access the system to manipulate his/her grades.

As discussed earlier in this guidebook, the agency must develop and disseminate clearly stated Internet/World Wide Web usage policies. These policies will add clarity to the tasks required of the network administrator. They should include:

- a password policy;
- an Acceptable Use Policy;
- anti-virus procedures;
- an e-mail policy;
- a remote access policy;
- an encryption policy;
- system audit procedures;
- confidentiality and data distribution procedures; and
- a copyright compliance policy.

> **The greatest security risks come from people inside the agency, not from outside hackers.**

Summary

- The agency should perform a security assessment to determine what measures need to be taken.

- System security is a complex enterprise that is best left to professionals rather than to high school faculty or technology staff. However, when resources dictate the use of teachers/technology coordinators to implement security, the provision of adequate professional development and written policies is critical.

- Hardware security includes creating a physical environment in which equipment is protected.

- Application and operating system software can be protected by using passwords and by eliminating access to those who have no need to use particular software.

- Many aspects must be addressed to ensure total network security, including the following:
  - qualified individuals must be hired to maintain networks;
  - appropriate tools must be used to monitor networks;
  - intrusion detection systems must be used; and
  - regular inspection and analysis of router audit logs must be implemented.

- Data integrity and security can be maintained through processes similar to those used for operating system security.

- Each computer connected to a network should be protected by anti-virus software.

- The transmission of data from one agency to another creates additional security risks that can be minimized through the use of standardized protocols, various encryption technologies, and digital signatures.

Conclusion

Interest in the development of academic web sites continues to grow as more and more homes become computer-friendly. The community wants to know what is going on in its schools, and parents want to keep track of the academic progress of their children. It is increasingly expected that, with the presence of the web, access to education agencies is to be available to students, teachers, and parents at all times.

The purpose of this guidebook is to provide an overview of the Internet and intra-agency networks, to discuss the development and standardization of World Wide Web sites, and to examine procedures that provide a secure environment for education agency networks and web sites.

Systematic technology planning is essential for every organization. Technology development is costly and complex and the development of a technology plan is difficult work, involving participation from all areas of the agency. Without a plan, the technology is still accessible, but its use may be haphazard and unduly expensive. If an agency has no plan at the outset, it is a certainty that a plan will be necessary later.

Education agencies should understand that there is no "one size fits all" plan for technology development or technology security. Each agency must develop an individualized plan that meets the specific needs of the organization. Guidebooks like this sometimes leave the impression that once a technology initiative is implemented, it is finished. Technology is never finished. Effective technology implementation involves a continuing professional development program, a plan to replace and/or redirect hardware and software, current virus protection, time allotted to evaluate existing policies/procedures, and an ongoing budget to accomplish all of these tasks.

This guidebook and a PowerPoint® presentation are available at http://nces.ed.gov/forum/. The PowerPoint® presentation may be modified to meet the needs of the agency.

What is the Internet?

The Internet is a decentralized network of networks. What does that mean? In computer terms, a network is a series of computers that are connected together to share information or resources. The Internet connects a variety of sites in a shared network. These sites may be universities, schools, government, and/or businesses. While these institutions are not directly connected to one another, they are electronically connected, which allows them to send information to one another. The Internet makes physical location much less important today than it once was. For example, students in Iowa can use the Internet to reference the Library of Congress right from their Iowa classroom, without going to Washington, DC. Moreover, the parents of a student at the local elementary school can receive information about homework from their child's teacher, without going to the school.

One of the great strengths of the Internet is its flexibility. Users can connect to the Internet through a single computer, through the local area network (LAN) in a single building, or through the wide area network (WAN) that connects the computers within a wider region (e.g., all of the computers in a school district). If the Internet connection is established through a LAN or WAN, then individual computers within that network will probably be routed through a main server that connects the network to the outside world. This routing creates efficiency, as the traffic from the numerous computers on the local network is organized and prioritized to make efficient use of the single connection to the Internet.

With a system as massive as the Internet, it would seem that there should be some central control governing computers and network traffic. As mentioned above, the network is almost entirely decentralized. There are no huge central computers controlling the Internet and monitoring its activity. Instead, the central core of the Internet consists of routers, which serve essentially the same function as postal sorting facilities: they read a recipient address (each computer has a unique address) and forward information along to another router that is closer to that address. Eventually, the "information package" gets to its destination.

While this system may sound inefficient, it works. An e-mail message may travel through 20 different routers on its way from the sender to the receiver, but the entire process actually takes only a second or two. The network is designed this way for a number of reasons, the most important of which is its high resistance to damage, even in times of war (the original network was designed by the military). If one router is destroyed, breaks, loses power, or otherwise ceases to function properly, traffic is simply rerouted around the hole in the network.

The Internet is also "interoperable" and "platform independent." Users of all different kinds of computers can view content, send information, and receive data on the Internet. E-mail sent from a Macintosh computer can be received and viewed on another Macintosh—or on a Windows PC, a Linux computer, or a UNIX machine. That means when web pages are written in one or more of a shared set of languages, the language(s) are interpreted almost identically on a variety of platforms.[1]

---

[1] These languages are interpreted almost identically. Different web browsers on different platforms often interpret data slightly differently (particularly data that do not comply with the appropriate standards). This may cause web pages to appear differently on different computers (or, in some cases, to not load at all).

How Does the Internet Work?

The Internet is often referred to as the *information superhighway,* which is a useful metaphor to explain how the Internet actually functions. One should think of the Internet as a superhighway that stretches around the world. On this superhighway, huge amounts of data are constantly traveling back and forth, as people request and send information from the many remote locations connected to the Internet.

In addition, there are numerous smaller information highways connected to the superhighway, like local routes that connect to the interstate. For example, if a person drives from Boston, Massachusetts, to Denver, Colorado, he or she would take a local road in Boston to the interstate highway; once in the Denver area, he or she would exit the interstate to a local road leading directly into Denver.

When an e-mail message travels along the Internet from a computer in Boston to a computer in Denver, what actually happens to it? The e-mail application (e.g., Outlook©, Pegasus©, etc.) will first attach a header to the e-mail message. The header is like an address on the outside of an envelope; it does not change the substance of the message, but it tells the delivery service (in the case of e-mail, the Internet) where the message needs to go.

When a user clicks on the send button of the e-mail application, a router receives the message and sends it on the local highway toward the superhighway. When the message gets to the superhighway, passing through a series of smaller highways on the way, another router directs it the right way. When it gets to the "off-ramp," another router intercepts it and directs it further along the way. Eventually, the e-mail reaches the server of the intended recipient and waits to be read in an electronic mailbox.

In reality, the Internet does not actually send the entire e-mail message as one package. Instead, it breaks the message up into a series of small packets, addresses them, and sends each of them individually. Each of these packets consists of a header and a little piece of the message. A single e-mail message may be broken up into a half dozen individual packets, which are separately routed. They may take slightly different paths to get to Denver, but once they are all there, the server at the receiving end reads the address in the header and puts the pieces back together. The recipient would never know it had been taken apart. (See appendix G, "Follow that Packet: Deep Down Security.")

Internet traffic does not consist only of e-mail. In fact, most Internet users browse the web for public files containing everything from pictures and small items of information to entire books. Web traffic is a big part of the total Internet traffic. When using a web browser, such as Internet Explorer™ or Netscape, information is retrieved from the Internet to be viewed on the user's desktop, at home or in the classroom. When connecting to a web site, the browser sends a short message to the site asking it to return all of the content for the page requested. The computer hosting the web site receives that message and returns a copy of the web page. When clicking on a link to another web site, the back and forth communication occurs each time.

Sometimes a web page takes a bit of time to "load," or show up on the screen. This is particularly true with a web page that has many pictures or symbols, called graphics. A file containing graphics that are much larger than the average e-mail message may cause this time lag. Just like e-mail messages, these files get broken up for the routing process—in the case of some web pages, they're broken into hundreds or thousands of packets that need to find their way to the person requesting the page.

There is another speed bump in the information superhighway. Millions of people are sending e-mails and web requests and are transferring files at the same time. Each of these "messages" is broken up into dozens, hundreds, or thousands of smaller packets, which are sent out over the Internet. At any given instant, literally hundreds of millions of packets are whizzing down the highway. Routers all over the world are constantly taking packets in and sending them out towards other routers closer to the packet's destination.

When too many of these packets are on the Internet, it slows everything down, just like a speed bump on an ordinary highway.

All of these packets whizzing back and forth are referred to, collectively, as network traffic. When there is too much traffic on any given road, or network, the traffic is rerouted—automatically—to a different but parallel highway or superhighway in order to bypass the congestion. The Internet, in fact, is not a single superhighway as the metaphor implies, but is rather a collection of dozens of parallel superhighways that provide an even greater capacity for traffic.

As important as it is to understand how information travels from one computer to another across the Internet, it is equally important (if not more so) to understand what happens to the Internet traffic when it gets closer to home. A basic understanding of how LANs function (see appendix B) is especially important for agency policymakers who must make decisions about web development and technology in general.

What is a Local Area Network?

A local area network (LAN) connects personal computers, printers, and other computer resources together within a building or campus. Many schools, offices, and even homes now have LANs. These networks allow printers, as well as documents and projects, to be shared. LANs also enable computers to talk to one another and are often used to share Internet access across all of the computers in a building or school.

Most LANs use wires, or cables, to connect computers and other peripheral devices. In most networks, a network cable (which generally looks like an oversized telephone cord) connects a computer to a network jack in the wall. Sometimes, in classrooms or business offices, many computers are connected to an intermediate hub or switch, not directly to the network jack. The hub or switch into which all of the computers are plugged is the device that is connected to the network jack. In both cases, the network jack is connected to a small router by another cable. Printers are also often shared using this method of hubs and switches.

Some LANs are now wireless. Wireless LANs are fundamentally the same as wired LANs, but the cabling is replaced by small "radios" that are contained inside the computers. Wireless LANs are generally somewhat slower than the wired networks, but they are much easier to set up and allow users to move their machines around without having to reconnect network cables.

Wireless LANs have moved into the mainstream in schools and classrooms during the last few years; however, it is important to note that security is much more difficult when using a wireless network (see chapter 6 of this guidebook for security recommendations). Additionally, the adoption of competing protocols is creating some confusion in the marketplace. Agencies need to select a wireless protocol with care, considering how the network can be upgraded and whether it is compatible with existing wireless protocols.

Where a LAN may connect all of the computers within a building or campus, a wide area network (WAN) connects multiple LANs. Many districts now have WANs connecting all of the schools within the district for the sharing of Internet access, selected files, or other resources.

What Are Servers, Routers, and Firewalls?

LANs often involve a number of different components, including a dizzying variety of servers, switches, routers, firewalls, and the like. This section provides descriptions of many of these items.

Servers

While servers often are spoken of in almost mystical tones, they are really just powerful computers running specialized software designed to share files, manage printers, or perform any other specialized task assigned. Most of these computers are powerful enough to do more than one thing at a time; for example, a single network server might be a file server, a print server, and a mail server simultaneously.

- *File server.* A file server is essentially the computer equivalent of a filing cabinet. Documents, spreadsheets, and other (computer) files are stored on a file server, just as paper documents are stored in a filing cabinet. The file server's job is to make those files available to computer users on the LAN and, when appropriate, allow the users to update the files.

- *Print server.* A print server is a piece of software or hardware that manages print jobs submitted by users. When a document is sent to a networked printer, the print server receives the job and queues it (puts it in line behind previously submitted jobs). When a job gets to the front of the queue, the print server sends it to the printer. It is not necessary to buy an individual printer for each personal computer. Users in classrooms or offices often share printers, since not everyone is typically printing at the same time. This option can save an agency a great deal of money.

- *Mail server.* The third common type of server is a mail server. The mail server acts as the conduit to the outside world as messages are sent and received. Some servers are set up so that all of the mail stays on the mail server until a user actively deletes it. In other configurations, the user is able to move the mail from the server to the desktop computer. This process, called "downloading," uses less space on the mail server.

Router

A router is a piece of equipment that acts as the interface between a local network and the Internet, by routing traffic from one to the other. A router may be a computer dedicated to managing the traffic of a WAN, or it may be a piece of software running on a computer that is configured for other tasks as well. Routers also may be used in LANs to route internal traffic.

Firewall

A critical component of any network is a firewall. A firewall in layman's terms is a wall that acts as a firebreak—it keeps a fire from spreading. In this sense, a computer firewall keeps a network secure from hackers (the "arsonists" of the Internet) by denying access to all or part of the network. Management of firewalls requires a great deal of expertise. While the network administrator must ensure that no unwanted traffic can enter the network from outside, a level of access to and from the Internet must be created that will permit authorized users to conduct their business safely and efficiently.

A solid, well-designed firewall is critical to ensure that only authorized users have access to a restricted network. Like routers and servers, firewalls are available as either hardware or software. Choosing a firewall for a particular network is an issue best addressed at the local level, after reviewing the options available. Firewalls and network security in general are discussed at length in chapter 6 of this guidebook.

Running Applications: Server vs. Desktop Computer

Advances in technology have blurred the distinctions between the computer on the desktop and a network server. Computing power has continued to grow exponentially—in fact, most users do not need all the computing power available to them (at least for now). The same is true of network servers, which have become so powerful that some network administrators run applications, in addition to the server software, from the network server, rather than installing applications directly on each of the computers

connected to the network. Servers are capable of managing a much greater workload today than they were in past years.

Running applications from a server has a number of advantages. One key advantage is in licensing, since it is much easier to track usage. Another is that local users are prevented from altering the configuration of applications, which can create software failure and cause problems for other users. In addition, it is much easier to upgrade software since only one copy needs to be upgraded, instead of upgrading one copy for each personal computer. Applications run from a network server, however, are often comparatively slower than applications running directly on a desktop computer.

Another benefit to server-run applications is the cost-saving use of *thin clients*. Thin clients are basic, low-cost computers with insufficient power to run sophisticated software applications, but with enough power to access applications installed on the server. By purchasing a single copy of an application that can run on a network, with licenses for multiple users, the organization can save the cost of multiple software copies and can purchase less powerful computers at a much lower cost. In addition, by instituting a thin client environment, older computers in schools have longer useful lives. In recent years, more and more LANs have incorporated thin clients for a variety of purposes.

In addition, more and more computer applications are written to take advantage of the web to run remotely. The user's desktop computer essentially acts as a "dumb" terminal, simply displaying the web pages broadcast by the server. The computing actually takes place on an Internet server, and users transmit their commands via the web page. This web-based model works best when users have high-speed Internet connections, as described in appendix C.

Computing today occurs on the desktop, on network servers, and Internet servers alike. The distinctions between the various types of computers and servers, in many cases, matter less and less. As computer and network transmission speeds improve, the differences will be even harder to grasp. The increasing complexities of computing and networking reinforce the need for agencies to employ the services of a qualified network administrator.

On the following page is a depiction of a sample classroom and school network configuration.

A Sample Classroom and School Network Configuration

Internet

Switch
Router

Firewall

Applications

Mail Server

Web Server

Switch Router

Switch Router

Printer

Printer

Classroom LAN

Classroom LAN

Classroom

Classroom

Classroom
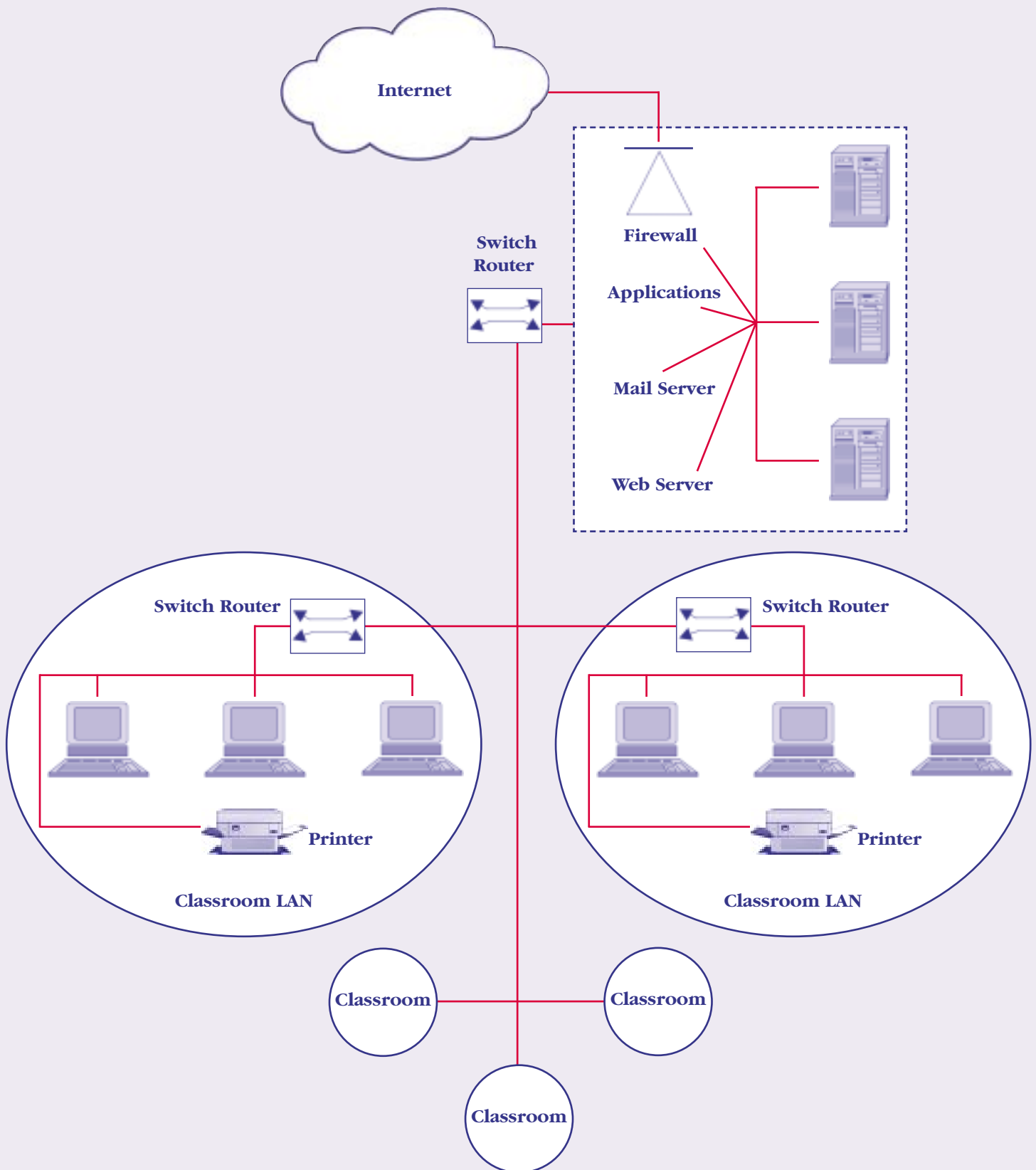
Connecting to the Internet

There are many different ways to connect to the Internet. Agencies can generally purchase several different kinds of on-ramps to the *information superhighway* based on their particular need. Depending on the kind of connection to the Internet, access to information may be fast or slow.

The key to Internet speed is *bandwidth.* Bandwidth refers to the amount of data transferred within a specified time. Greater bandwidth increases the speed of data transfer. A general overview of the various types of Internet connections is listed below, starting with the slowest (smallest bandwidth) and moving up to the faster (greater bandwidth) technologies. Cost and service quality can vary widely. Use of a competitive bid process, with an appropriate Request for Proposal (RFP), can better enable agencies to obtain needed service while controlling cost. In other words, the agency should not commit to service from a provider based on advertisements.

Acronyms and abbreviations referenced in this appendix are defined in the glossary. A reference table is provided at the end of this appendix for quick comparison of the various Internet connection options discussed below.

Internet Service Providers

Internet Service Providers (ISPs) provide the portals, or access, that allow computer users to connect to the Internet. There are numerous ways for education agencies to connect with an ISP. Before selecting an ISP, the agency should determine its needs for bandwidth, speed, and services.

The agency should secure the services of an ISP through the RFP process. Using the RFP process, the ISP should be required to identify the available connection speed and the reliability of the system, sometimes measured by the amount of time the ISP's services were down during the previous 6 months. Although most ISPs will advertise a high connection speed, the agency should determine whether the full bandwidth is available at all times by requesting an assessment of the provider's typical bandwidth and connection speed at different times of the day and on different days of the week. The chief technology officer or technology director should review any ISP proposal. Following are descriptions of the various Internet connections available.

Dial-Up

Dial-up services connect to the Internet using modems over a traditional telephone line. The vast majority of Internet users connect to the Internet from home via dial-up service. The maximum connection speed is 56 kilobits per second (Kbps), which is slow when supporting bandwidth-intensive services, such as video conferencing or streaming video. Dial-up service is typically sufficient for using web and e-mail applications. It is not recommended for multiple users, such as a number of students, who need to access the Internet at the same time. Dial-up service is available almost everywhere in the United States and is the least expensive way of connecting to the Internet/World Wide Web.

ISDN

Developed and marketed through the 1980s and early 1990s, the Integrated Services Digital Network (ISDN) was the telephone company's first attempt at providing faster online services. As with dial-up service, ISDN is generally insufficient for serving a large number of users with the same connection. The service provides up to 128 Kbps, approximately twice the speed of dial-up. ISDN tends to be much more expensive than dial-up, costing generally $100 to $300 per month. For the most part, DSL technology has replaced ISDN; however, in some areas where DSL is not available, ISDN may be the best option. If available, most of the other services mentioned in this appendix provide greater capacity at lower cost than ISDN.

DSL

Digital Subscriber Line (DSL) technologies have largely replaced ISDN service as the product telephone companies want consumers to use when connecting to the Internet. Like dial-up service, DSL connects to the Internet over ordinary copper telephone lines, but is faster—at rates of 1.5 to 6.1 megabits per second (Mbps)—enabling continuous transmission of video and audio. DSL service is primarily marketed to home and small business users, but the service is adequate to meet the needs of education agencies. While it does not have the same quality of service in terms of speed or support that dedicated fiber optic lines typically provide, DSL is much more affordable. DSL is available in much of the United States, particularly in urban areas. Commercial DSL service generally runs from $100 to $250 per month, but can run significantly higher.

DSL service quality can vary from area to area and from service provider to service provider. Additionally, the speed of access to the Internet depends on the distance between the user and the DSL relay station.

Cable Modems

Cable modems have become, in recent years, the most popular broadband technology for home computer users. The cable modem uses the same coaxial cable that carries cable TV signals for high-speed data transmission. While not as robust as fiber optic connections, cable modems can provide similar quality service at a fraction of the cost. The quality of a cable modem connection, however, is dependent on the overall quality of the cable modem provider's network, and the more people accessing the provider's network at the same time, the slower each individual's connection to the Internet will be. Speed ranges from under 1 to 8 Mbps; costs are generally $100 to $250 per month for commercial users.

Because of the historically strong connection between education and the cable television community, many schools are using cable modems. When contracting to provide cable service to a city or county, the cable company typically makes the commitment to provide one cable connection and one modem to each school within the service area of the cable company. There are cases, however, in which cable companies have provided additional services.

Higher Bandwidth Connections (including fiber optics)

Many businesses and schools today connect to the Internet through larger cables, typically referred to as T1 (copper wire), T3 (coaxial cable or fiber optic cable), or OC3c (fiber optic) connections. These services are widely available, are highly flexible, and provide high quality, fast broadband service. Costs are comparatively high and vary widely from area to area. In urban areas, T1 connections (providing 1.5 Mbps) are generally available

for approximately $200 to $500 per month. In rural areas, the same connection usually costs much more. Larger T3 and OC3c connections, which provide 45 Mbps and 155 Mbps, respectively, generally cost several thousands of dollars per month in urban areas and tens of thousands of dollars per month in rural areas. Depending on the bandwidth needs of the school or district, it may be more sensible to utilize a less expensive connection.

For some agencies, a more feasible option in the T-carrier system may be a "fractional" T1 line, which utilizes a portion of the T1. Fractional T1 lines are available to meet almost any speed requirement for a reduced price. This option makes sense for those agencies that may not need a full T1 line today, but might need increased bandwidth in the future. In addition, upgrading fractional T1 to use more of the T1 line can usually be done without purchasing new hardware.

Larger organizations, such as state government agencies or large school districts, may require the faster OC3c connection. These high-speed connections are not always available and, as mentioned, can cost tens of thousands of dollars per month. Where these networks exist, however, states (or counties or large districts) may be able to divide the bandwidth, according to the needs of smaller districts or schools. By doing this, the cost of connecting to the Internet could be reduced for smaller agencies or schools. Districts or schools should, when considering which kind of connectivity to purchase, determine if there is a preexisting network to which they can connect.

Satellite

Some larger agencies have considered buying space on a satellite to upload and download files. While the cost of transmitting information over wires would be removed, satellite reliability is debatable. Weather (such as rain) or even sunspots can affect satellite transmission. Additional information on satellite transmission can be found at *http://www.geocities.com/al_chong/*.

Cellular Wireless

Traditionally, Internet access over cellular telephone networks has been slow and somewhat unreliable. Wireless technology, however, is coming of age, and new, significantly faster Internet connection services are offered throughout the United States. While these "third generation wireless" services (generally referred to as 3G services) are not necessarily suitable for building use, they may suit the needs of individuals within the agency as they maintain contact with each other during the workday. Already, cellular phones are replacing "walkie-talkies" in many secondary schools. It is still too soon to tell how much these services will cost, but they will probably be metered, with cost depending upon the amount of usage.

Fixed Wireless

Fixed wireless refers to the operation of wireless devices in a fixed location. Unlike mobile wireless devices, which are battery powered, fixed wireless devices are electrically powered. The basic idea behind fixed wireless is that the traditional wired connection (e.g., fiber optic, telephone line, or cable TV line) is replaced by a high-speed wireless connection. Depending on the technology, bad weather (such as rain) can significantly interfere with fixed wireless services. This service is usually most attractive in communities where traditional wired connections are not available; however, the technology is also suitable for urban areas. Fixed wireless speed varies considerably, from under 1 Mbps to upwards of 15 Mbps. Cost also varies widely.

A summary of the types of Internet connection options is provided on the next page in a quick reference format.

Internet Connections—Quick Reference

Service type	Speed	Strengths	Weaknesses
Dial-Up	<56 Kbps	• Inexpensive • Widely available; connection is made through the telephone line • Useful when only one computer is connected to the Internet	• Only one computer at a time can use the connection • Comparatively slower speed makes using graphics (pictures) difficult
ISDN	64–128 Kbps	• Faster than dial-up connections • Graphics can be transmitted more easily than with dial-up connections	• Support by service providers is decreasing • Cost can be high
DSL	256 Kbps–10$^+$ Mbps	• Inexpensive • More useful when a limited number of computers are connected to the Internet	• Limited by physical distance from the service provider • Limited number of computers can connect before speed is degraded (graphics will load very slowly)
Cable Modem	1–8 Mbps	Connectivity to more than one computer can be developed from one cable connection	• Access to cable systems is usually determined by agreements between vendors and city/county government • The more connections on the cable, the slower the system • Individual e-mail accounts are usually expensive
Higher Bandwidth Connections	1.5–155$^+$ Mbps	• Allows for multiple connections • Speed of connectivity only limited by the number of users on the Internet • Expandable	• Expensive • Connection is complex
Satellite	350 Kbps$^+$	Available in rural areas where other options may not be available	• Expensive • Upload speed may be slow • Usually requires additional phone line to communicate with the service provider
Cellular Wireless	<28 Kbps (currently) Approx. 200 Kbps (3G)	Useful for individual connectivity only	Not an option for schools or classrooms
Fixed Wireless	1–15 Mbps	Useful in areas where there are no wires	• Very limited availability • Bad weather can interfere with data transmission

bps = bits per second
Kbps = kilobits per second (1 Kbps = 1,000 bps)
Mbps = megabits per second (1 Mbps = 1,000 Kbps = 1,000,000 bps)
Gbps = gigabits per second (1 Gbps = 1,000 Mbps = 1,000,000 Kbps = 1,000,000,000 bps)

Internet Addresses and Domains

Everyone who has watched television, listened to the radio, or surfed the web in the last half-dozen years is familiar with Internet addresses or, more precisely, Uniform Resource Locators (URLs). In fact, these addresses have become so commonplace that many companies now include them, often in place of telephone numbers, as the primary contact information in their advertisements.

An Internet address is actually the verbal translation, or domain name, of a numeric Internet Protocol (IP) address, which represents a unique computer location on the Internet. For example, when the domain name *nces.ed.gov* is keyed into a web browser, the browser asks a server for the actual IP address (in this case, 165.224.221.98), which tells the browser how to get to the site. Users generally are not even aware that these numbers exist and, for almost all operations, use the shorthand Internet address rather than the numeric IP address.

An Internet address is broken into several different segments separated by periods. The address segments are read in backwards order to determine the location of the server. The first component of an Internet address is the top-level domain (TLD), which identifies the nature of the address owner's business. The TLD most people are familiar with is *.com* ("dot com"), short for *commercial*. In addition to *.com*, there are several other generic TLDs, including *.org, .edu,* and *.net*, as well as country-specific TLDs such as *.us* and *.uk*. The rules for using a particular TLD vary; for example, virtually anyone can get a *.com* address, but, for the most part, *.edu* addresses are available only to institutions of higher education.

The following table identifies a few of the TLDs that are currently available. New domains are being added constantly.

Top-Level Domains	
	Restrictions
.com	None – Anyone can register. Originally restricted to for-profit companies.
.net	None – Anyone can register. Originally for network infrastructure Companies only.
.org	None – Anyone can register. Originally for nonprofits only.
.edu	Limited to institutions of higher education (except for grand-fathered institutions).
.gov	United States federal and state governments only.
.jp	Japan's country code. Limited to organizations, institutions, and individuals in Japan.

Top-Level Domains *(continued)*	
	Restrictions
.name	None – Available to anyone who wants to register a *name* domain (e.g., john_smith).
.mil	United States military only.
.kids	For noncommercial children's content. Not yet available.
.biz	None – Anyone can register.
.info	None – Anyone can register.
.us	None – Anyone can register. The *.us* domain is the United States country code. Originally limited to a geographic system of naming (*www.name.state.us*), but being reformed.
.tv	Tuvalu's country code (an island nation in the South Pacific). No restrictions. Widely used for television-related industry.

The second-level domain (SLD) is the portion of the URL that identifies the owner of the IP address. The rules for SLDs are even less regulated than those for TLDs. Some TLDs, such as *.com*, have no restrictions at the second level, so virtually anything can be registered. Others have significant SLD restrictions, such as *.us*, which requires state identifiers at the second level.

Starting from the TLD and working backwards, the Internet address provides information about the address owner. Using the example *nces.ed.gov*, it can be determined that the address owner (TLD) is

(1) *.gov*, meaning it is affiliated with the U.S. government;

(2) *.ed.gov*, meaning it is part of the U.S. Department of Education (SLD); and

(3) *nces*, the National Center for Education Statistics at the U.S. Department of Education.

Similar rules apply as more and more domains are added to an address. The drawback to increasing the levels of information within an Internet address is that the address can become unwieldy. The more levels in the address, the more difficult it is to remember. School districts have been traditionally sequestered in the *.us* domain, and they consequently often have web addresses that can be hard to recall from memory.

When choosing a domain name, one should exercise judgment in determining whether a short and simple or longer and more descriptive name is appropriate, and then check to see if it is available for use. Companies that sell domain names for profit quickly snatch up simple domain names. To check the availability of a domain name or to register a name, one should go to any online domain registrar, such as *www.register.com* or

www.networksolutions.com. The cost of registering and maintaining a domain name is approximately $35 per year.

Multiple addresses/domain names can be registered for a single web site for a variety of reasons. For example, General Electric, for access to the same site, registered both *www.generalelectric.com* and *www.ge.com.* An education agency or district can likewise register multiple addresses for its web site; however, only a single address should be advertised to minimize confusion among staff, parents, and the public. A district may choose to register different addresses in order to convert a long domain name to a shorter one or to guarantee that an alternate address will remain available for use by the district at a future date. More importantly, the registration of potentially competing or confusing addresses prevents them from being used by someone else.

Policies and Procedures (Samples): Acceptable Use Policy

(Rochester School Department, Rochester, New Hampshire)

Acceptable Use of Internet and Other Electronic Resources

The [Education Agency Name] recognizes the value of computer and other electronic resources to improve student learning and enhance the administration and operation of its schools. To this end, the [Governing Body Name] encourages the responsible use of computers; computer networks, including the Internet; and other electronic resources in support of the mission and goals of the [Education Agency Name] and its schools.

Because the Internet is an unregulated, worldwide vehicle for communication, information available to staff and students is impossible to control. Therefore, the [Governing Body Name] adopts this policy governing the voluntary use of electronic resources and the Internet in order to provide guidance to individuals and groups obtaining access to these resources on [Education Agency Name]-owned equipment or through [Education Agency Name]-affiliated organizations.

[Education Agency Name] Rights and Responsibilities

It is the policy of the [Education Agency Name] to maintain an environment that promotes ethical and responsible conduct in all online network activities by staff and students. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of the network. Within this general policy, the School Department recognizes its legal and moral obligation to protect the well-being of students in its charge. To this end, the [Education Agency Name] retains the following rights and recognizes the following obligations:

1. To log network use and to monitor fileserver space utilization by users, and assume no responsibility or liability for files deleted due to violation of fileserver space allotments.

2. To remove a user account on the network.

3. To monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.

4. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to [Education Agency Name]-owned equipment and, specifically, to exclude those who do not abide by the [Education Agency Name]'s acceptable use policy or other policies governing the use of school facilities, equipment, and materials. [Education Agency Name] reserves the right to restrict online destinations through software or other means.

5. To provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing online communications.

Staff Responsibilities

1. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the [Education Agency Name].

2. Staff should make reasonable efforts to become familiar with the Internet and its use so that effective monitoring, instruction, and assistance may be achieved.

User Responsibilities

Use of the electronic media provided by the [Education Agency Name] is a privilege that offers a wealth of information and resources for research. Where it is available, this resource is offered to staff, students, and other patrons at no cost. In order to maintain the privilege, users agree to learn and comply with all of the provisions of this policy.

Acceptable Use

1. All use of the Internet must be in support of educational and research objectives consistent with the mission and objectives of the [Education Agency Name].

2. Proper codes of conduct in electronic communication must be used. In news groups, giving out personal information is inappropriate. When using e-mail, extreme caution must always be taken in revealing any information of a personal nature.

3. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.

4. All communications and information accessible via the network should be assumed to be private property.

5. Subscriptions to mailing lists and bulletin boards must be reported to the system administrator. Prior approval for such subscriptions is required for students and staff.

6. Mailing list subscriptions will be monitored and maintained, and files will be deleted from the personal mail directories to avoid excessive use of fileserver hard-disk space.

7. Exhibit exemplary behavior on the network as a representative of your school and community. Be polite!

8. From time to time, the [Education Agency Name] will make determinations on whether specific uses of the network are consistent with the acceptable use practice.

Unacceptable Use

1. Giving out personal information about another person, including home address or phone number, is strictly prohibited.

2. Any use of the network for commercial or for-profit purposes is prohibited.

3. Excessive use of the network for personal business shall be cause for disciplinary action.

4. Any use of the network for product advertisement or political lobbying is prohibited.

5. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.

6. No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.

7. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

8. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.

9. The unauthorized installation of any software, including shareware and freeware, for use on [Education Agency Name] computers is prohibited.

10. Use of the network to access or process pornographic material, inappropriate text files (as determined by the system administrator or building administrator), or files dangerous to the integrity of the local area network is prohibited.

11. The [Education Agency Name] network may not be used for downloading entertainment software or other files not related to the mission and objectives of the [Education Agency Name] for transfer to a user's home computer or other personal computer. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the [Education Agency Name].

12. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).

13. Use of the network for any unlawful purpose is prohibited.

14. Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.

15. Playing games is prohibited unless specifically authorized by a teacher for instructional purposes.

16. Establishing network or Internet connections to live communications, including voice and/or video (relay chat), is prohibited unless specifically authorized by the system administrator.

Disclaimer

1. The [Education Agency Name] cannot be held accountable for the information that is retrieved via the network.

2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

3. The [Education Agency Name] will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.

4. The [Education Agency Name] makes no warranties (expressed or implied) with respect to:

    - The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;

    - Any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.

5. The [Education Agency Name] reserves the right to change its policies and rules at any time.

Policies and Procedures (Samples): Technology Resource Use Agreement

(Rochester School Department, Rochester, New Hampshire)

## [Education Agency Name]

User Agreement (To be signed by all adult users and student users above grade 5)

I have read, understand, and will abide by the above Acceptable Use Policy when using computer and other electronic resources owned, leased, or operated by the [Education Agency Name]. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

_____
User Name (please print)

_____
User Signature   Date

Parent Agreement (To be signed by parents of all student users under the age of eighteen)

As parent or guardian of this student, I have read the Acceptable Use Policy. I understand that this access is designed for educational purposes. [Education Agency Name] has taken reasonable steps to control access to the Internet, but cannot guarantee that all controversial information will be inaccessible to student users. I agree that I will not hold the [Education Agency Name] responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my child to use network resources, including the Internet, that are available through [Education Agency Name].

_____
Parent Name (please print)

_____
Parent Signature   Date

Policies and Procedures (Samples): Electronic Mail Policy

(Rhode Island Department of Education)

User Responsibilities

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal. You should understand the following:

The agency provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies, and partner organizations.

When using the agency's electronic mail facilities you should comply with the following guidelines.

If you are in any doubt about an issue affecting the use of electronic mail, you should consult the IT Services Manager.

Any breach of the agency's Electronic Mail Policy may lead to disciplinary action.

DO

✔ Do check your electronic mail daily to see if you have any messages.

✔ Do include a meaningful subject line in your message.

✔ Do check the address line before sending a message and check you are sending it to the right person.

✔ Do delete electronic mail messages when they are no longer required.

✔ Do respect the legal protections to data and software provided by copyright and licenses.

✔ Do take care not to express views that could be regarded as defamatory or libelous.

✔ Do use an "out of the office assistant" to automatically reply to messages when you are not available.

DO NOT

✘ Do not print electronic mail messages unless absolutely necessary.

✘ Do not expect an immediate reply; the recipient might not be at their computer or could be too busy to reply straight away.

✘ Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.

✘ Do not use electronic mail for personal reasons.

✘ Do not send excessively large electronic mail messages or attachments.

DO NOT *(continued)*

   ✘ Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to several people.

   ✘ Do not participate in chain or pyramid messages or similar schemes.

   ✘ Do not represent yourself as another person.

   ✘ Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive, or libelous.

Please note the following:

- All electronic mail activity is monitored and logged.

- All electronic mail coming into or leaving the Company is scanned for viruses.

- All the content of electronic mail is scanned for offensive material.

Policies and Procedures (Samples): Dial-In Access Policy

(Rhode Island Department of Education)

1. Purpose

The purpose of this policy is to protect [Agency Name]'s electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

2. Scope

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3. Policy

[Agency Name] employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate, or agency, network. Dial-in access should be strictly controlled, using one-time password authentication. Dial-in access should be requested using the corporate account request process.

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to [Agency Name] is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and [Company Name] are literal extensions of [Agency Name]'s corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect [Agency Name]'s assets.

Analog and non-GSM digital cellular phones cannot be used to connect to [Company Name]'s corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to [Agency Name]'s network. For additional information on wireless access to the [Agency Name] network, consult the *Wireless Communications Policy.*

Note: Dial-in accounts are considered "as needed" accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months, the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policies and Procedures (Samples): Password Policy

(Rhode Island Department of Education)

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of [Agency Name]'s entire corporate network. As such, all employees (including contractors and vendors with access to [Agency Name] systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any [Agency Name] facility, has access to the [Agency Name] network, or stores any non-public [Agency Name] information.

4. Policy

4.1 General

A. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

B. All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

C. Each successive password must be unique. Re-use of the same password will not be allowed.

D. Passwords must be a minimum of eight (8) characters long.

E. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

F. Passwords must not be inserted into e-mail messages or other forms of electronic communication.

G. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

H. All user-level and system-level passwords must conform to the guidelines described below.

I. Passwords should never be written down or stored online.

4.2 Standards

A. General Password Construction Guidelines

Passwords are used for various purposes at the [Agency Name]. Some of the more common uses include: user-level accounts, web accounts, e-mail accounts, screen saver protection, voice-mail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

1. Poor, unacceptable passwords have the following characteristics:

   ✘ The password contains fewer than eight characters

   ✘ The password is a word found in a dictionary (English or foreign)

   ✘ The password is a common usage word such as:

   - Names of family, pets, friends, co-workers, fantasy characters, etc.
   - Computer terms and names, commands, sites, companies, hardware, software
   - Acronyms for the agency or city.
   - Birthdays and other personal information such as addresses and phone numbers
   - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   - Any of the above spelled backwards
   - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2. Strong (acceptable) passwords have the following characteristics:

   ✔ Contain both upper and lowercase characters (e.g., a-z, A-Z)

   ✔ Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

   ✔ Are at least eight alphanumeric characters long

   ✔ Are not a word in any language, slang, dialect, jargon, etc.

   ✔ Are not based on personal information, names of family, etc.

   ✔ Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

   NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for [Agency Name] accounts as for other non [Agency Name] access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for the various [Agency Name] access needs. For example, select one password for the E-mail systems and a separate password for network systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share agency passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential [Agency Name] information.

If someone demands a password, refer them to this document or have them call someone in the Office of Network and Information Systems.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the Office of Network and information Systems and change all passwords.

The Office of Network and Information Systems or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups;
- should not store passwords in clear text or in any easily reversible form;
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password, and
- should support TACACS+ , RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the [Agency Name] networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all and the private key that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning."

All of the rules above that apply to passwords apply to passphrases.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action and loss of network privileges.

6. Definitions

Terms/Definitions

Application Administration Account: Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

World Wide Web Consortium: Web Content Accessibility Guidelines

(http://www.w3.org/)

Guideline 1:

Provide equivalent alternatives to audio and visual content. (Provide content that, when presented to the user, conveys essentially the same function or purpose as auditory or visual content.)

Guideline 2:

Do not rely on color alone. (Ensure that text and graphics are understandable when viewed without color.)

Guideline 3:

Use markup and style sheets and do so properly. (Mark up documents with the proper structural elements. Control presentation with style sheets rather than with presentation elements and attributes.)

Guideline 4:

Clarify natural language usage. (Use markup that facilitates pronunciation or interpretation of abbreviated or foreign text.)

Guideline 5:

Create tables that transform gracefully. (Ensure that tables have necessary markup to be transformed by accessible browsers and other user agents.)

Guideline 6:

Ensure that pages featuring new technologies transform gracefully. (Ensure that pages are accessible even when newer technologies are not supported or are turned off.)

Guideline 7:

Ensure user control of time-sensitive content changes. (Ensure that moving, blinking, scrolling, or auto-updating objects or pages may be paused or stopped.)

Guideline 8:

Ensure direct accessibility of embedded user interfaces. (Ensure that the user interface follows principles of accessible design: device-independent access to functionality, keyboard operability, self-voicing, etc.)

Guideline 9:

Design for device independence. (Use features that enable activation of page elements via a variety of input devices.)

Guideline 10:

Use interim solutions. (Use interim accessibility solutions so that assistive technologies and older browsers will operate correctly.)

Guideline 11:

Use W3C technologies and guidelines. (Use W3C technologies, according to specification, and follow accessibility guidelines. Where it is not possible to use a W3C technology, or doing so results in material that does not transform gracefully, provide an alternative version of the content that is accessible.)

Guideline 12:

Provide context and orientation information. (Provide context and orientation information to help users understand complex pages or elements.)

Guideline 13:

Provide clear navigation mechanisms. (Provide clear and consistent navigation mechanisms—orientation information, navigation bars, a site map, etc.—to increase the likelihood that a person will find what he or she is looking for at a site.)

Guideline 14:

Ensure that documents are clear and simple. (Ensure that documents are clear and simple so they may be more easily understood.)

Follow That Packet: Deep Down Security

The information in this appendix describes how a secure local area network receives a "packet" from the Internet. The following security information is intended for the individuals within the education agency who already have a basic understanding of computer and network technology.

The Internet Service Provider (ISP) routes the packet that addressed to the agency from the Internet to the agency's border router. The border router typically runs a routing protocol such as BGP, EIGRP, OSPF, RIP, etc. The agency's ISP should install access control lists on this device to prevent access to anyone other than the Network Operating Center (NOC) servers and hosts. This device should also prevent the routing of RFC1918 address spaces (unroutable IP addresses: Class A 10.0.0.0–10.255.255.255 [10/8 prefix], Class B 172.16.0.0–172.31.255.255 [172.16/12 prefix], Class C 192.168.0.0–192.168.255.255 [192.168/16 prefix]).

From the border router, the packet arrives at the agency's edge router. Security processes to be addressed at the edge router are similar to those addressed at the ISP's border router. The difference is that the agency controls the configuration of the edge router. Processes to consider for edge router configuration include the following:

- ingress and egress filtering (to prevent IP spoofing);
- black hole routing for those address spaces the agency feels are necessary by interpreting the logs from the agency's intrusion detection system (addressed later);
- access control lists to prevent others from accessing Telnet or secure shell (SSH) sessions on the agency's router;
- username/password validation through Local, TACACS+, RADIUS, or Authentication, Authorization, and Accounting (AAA) to allow only authorized individuals to access the edge router;
- encrypted configuration passwords;
- firewall feature configuration as part of the router configuration (e.g., port and protocol blocking);
- proper Network Address Translation (NAT), Port Address Translation (PAT), and static addressing configuration if not handled on a separate firewall;
- disabling of built-in http server services should they exist;
- disabling of proprietary "neighbor" communication protocols; and
- disabling of all protocols and services not necessary for business operations.

From the edge router the packet travels to the outside switch. The switch is positioned at this location in the system to provide the flexibility to attach outside hosts and the ability to accomplish port monitoring with devices such as Content Filtering Servers (CFS) or Intrusion Detection Systems (IDS). The following items should be included in the configuration of the outside switch:

- access control lists to limit access to the Telnet or SSH sessions to individual network management hosts authorized to effect changes to the switch;

- username/password validation through Local, TACACS+, RADIUS, or AAA authentication to allow only authorized individuals to access the outside switch;
- disabling of proprietary "neighbor" communication protocols;
- enabling of port monitoring for IDS monitor, if installed;
- enabling of port monitoring for Internet CFS, if installed; and
- hard code port speed and duplex, if necessary.

It is highly recommended that an IDS monitor be installed as an attached device to the outside switch. This device monitors the arrival of packets at the network door, which in a properly secured system is the only entryway into the network. The IDS monitor can detect attempts to gain access to the agency's network, to map the network (through port scans), or to initiate denial of service (DoS) attacks against the network. The agency should evaluate the IDS data results to effect changes as needed to the edge router and firewall systems.

If there are other gateways into and out of the network, the edge router should be configured at each place according to the recommendations above. Each gateway should have a firewall and should be monitored by an IDS in addition to router audit log monitoring.

In addition to the IDS, some Internet CFS solutions can be installed at the edge router. In a manner similar to that of the IDS, the CFS device looks at every packet requested from the Internet and identifies any improper requests based on a defined list of improper sites. The improper request is denied and a Transmission Control Protocol (TCP) reset is sent back to the server. With this type of content filter, the CFS could be set to redirect an "inappropriate" user request to an internal (intranet) web server. The web server could send information, including the Acceptable Use Policy, back to the person who made the original request.

From the switch, the packet travels to the outside interface of the firewall. This is the last defense point. The network firewall should be configured to deny all inbound requests to the agency's internal network. The only accepted communication should be those packets bound for public servers (e.g., web, mail, etc.) residing on the Demilitarized Zone (DMZ) segment of the Local Area Network (LAN). Acceptable communication should be limited to IP address ranges, protocols, and ports suitable for the individual application on the individual server. All other inbound access should be denied. Other areas for consideration include the following:

- deny all inbound requests to the agency's internal network with exceptions noted below;
- allow only those addresses, protocols, and ports required to meet the needs of the application and allow them *only* on the DMZ segment;
- configure NAT, PAT, and static addressing as appropriate to suit the agency's needs;
- use access control lists to limit access to the Telnet or SSH sessions to those individual network management hosts authorized to effect changes to the switch and to the firewall;
- use username/password validation through Local, TACACS+, RADIUS, or AAA authentication to allow only authorized individuals to access the outside interface of the firewall;
- use RFC1918 (unroutable) address spaces, logically arranged, inside the firewall;
- place all internal hosts and servers on the most secure (internal segment) of the firewall;
- place all publicly accessible servers on the DMZ segment of the firewall;

- configure only the specific IP addresses and specific protocols and ports (e.g., Open Database Connectivity [ODBC]) of publicly accessible servers on the DMZ to communicate with any specific server on the internal network;

- configure communication to Internet content filtering, if required; and

- configure fail-over services, if enabled.

All instructional functions and student research hosts should reside on the DMZ segment of the network. All publicly accessible hosts on this segment or a lower security segment (e.g., DMZ1, DMZ2) should be installed. Such hosts may include web servers, File Transfer Protocol (FTP) servers, e-mail servers, etc. Administrative hosts on the DMZ segment should not be installed. Further segregation of student segments of publicly accessible servers can be accomplished in this manner.

Administrative hosts and servers hosting administrative applications, databases, file servers, print servers, and data should reside on the inside segment of the LAN.

For both the DMZ segment and the inside segment of the LAN, network monitoring tools, packet sniffers, and other such tools should be utilized to analyze the performance of the network and to ensure that the network is able to maintain adequate bandwidth and services. These tools can be handheld devices, such as client software installed on a monitoring station, or they can be web-based. To maximize security, caution should be exercised when using Simple Network Management Protocol (SNMP) tools.

Additionally, appropriate network monitoring and notification tools should be installed to alert assigned personnel to important events, such as device failures and intrusion incidents.

References

National Forum on Education Statistics (2001).
   Technology @ Your Fingertips. Washington, DC: U.S. Department of Education.

National Forum on Education Statistics (1998).
   Safeguarding Your Technology. Washington, DC: U.S. Department of Education.

National Forum on Education Statistics (2003).
   Technology in Schools. Washington, DC: U.S. Department of Education.

National Forum on Education Statistics
   http://nces.ed.gov/forum/publications
   The documents listed above are available at the Forum web site.

Educational Leadership
   "Schools and the Law: Copyright 101," Vol. 59, No. 4, Dec 2001/Jan 2002
   http://www.ascd.org/readingroom/edlead/0112/frame0112el.html

"Internet Access in U.S. Public Schools and Classrooms 1994-2001,"
   Kleiner and Farris, NCES publication # 2002-029
   http://nces.ed.gov/pubsearch

West Virginia Department of Education
   http://wvde.wv.us/disclaimer.html
   An example of a web site disclaimer.

Guidelines and Regulations
Accessibility (Section 508) final regulations
   http://www.access-board.gov/sec508/508standards.htm

Children's Internet Protection Act (CIPA)
   http://www/si.universalservice.org/CIPAfaq.asp
   These facts on CIPA are presented at the e-rate web site.

Copyright law (United States Copyright Office)
   http://www.loc.gov/copyright/title17/

Family Education Rights and Privacy Act (FERPA)
   http://ed.gov/offices/OM/fpco/ferpa

Individuals with Disabilities Education Act (IDEA)
   http://www.ed.gov/offices/OSERS/Policy/IDEA

HIPAA (Health Insurance Portability and Accountability Act)
   http://www.hcfa.gov/medicaid/hipaa/
   http://hippo.findlaw.com/hipaa.html

Section 508 and W3C Accessibility Guidelines
   http://www.cast.org/Bobby/
   This site contains a free test for web page compliance.

World Wide Web Consortium (W3C)
> *http://w3c.org*
> W3c has accepted guidelines and initiatives to optimize the use of the web.
> *http://www.w3c.org/WAI*
> Web Accessibility Initiative development work is described here.
> *http://www.w3c.org/TR/1999/WAI-WEBCONTENT-19990505/*
> The actual accessibility initiative is at this site.

Selected Security Resources

Carnegie Mellon University Computer Emergency Response Team (CERT")
> *http://www.cert.org/*
> A web site that reviews network vulnerabilities.

E-SECURE-DB IT Security Information Database
> *http://www.e-secure-db.us/dscgi/ds.py/View/Collection-226*
> A database of viruses and IT information on how to prevent, detect, and recover from virus attacks.

IETF (Internet Engineering Task Force)
> *http://www.ietf.org* and *http://www.rfc-editor.org/*
> IETF is the standards body that defines and maintains protocol standards for the Internet. These sites are used as references for protocol standards and to track emerging technologies that are becoming standards.

National Infrastructure Protection Center
> *http://www.nipc.gov/*
> *http://www.nipc.gov/cybernotes/cybernotes.htm*
> *http://www.nipc.gov/sites.htm*
> The NIPC provides timely warnings of international cyber threats, comprehensive analysis, and law enforcement investigation and response with links to other security-related agency web sites

National Security Agency
> *http://www.nsa.gov/snac/index.html*
> Security recommendation guides

Packet Storm
> *http://packetstorm.security.com/*
> This site is an excellent resource for network security news, vulnerability announcements, and security tools.

Security Focus
> *http://www.securityfocus.com/*
> This is a good site for security news and vulnerability information. There is not much information about routers, but it gives some advice on how to forestall certain attacks by using routers.

System Administration, Audit and Networking Organization
> *http://www.sans.org/top20/*
> This site describes the 20 most critical Internet security vulnerabilities.

These references were current at the time of publication; however, the authors cannot guarantee that the sites will be available in the future. The online version of the guidebook will be updated. Readers finding expired web links are asked to search the site for the information requested, to contact the web site owners, and to communicate with the guidebook authors at *http://nces.ed.gov/forum.*

Acceptable Use Policy (AUP): A policy designed to describe the ways in which a computer or network may be used. AUPs usually include explicit statements about the required procedures, rights, and responsibilities of a technology user. User agreement to all AUP stipulations as a condition of system use should be certified on the AUP by the user's signature.

Application: A computer program used to accomplish specific tasks not related to the computer itself (e.g., word processors, spreadsheets, accounting systems).

Asynchronous Transfer Mode (ATM): ATM is the name given to a network technology based on transferring data in *cells* or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video**,** audio, and computer data over the same network, while ensuring that no single type of data dominates the line.

ATM: See Asynchronous Transfer Mode.

AUP: See Acceptable Use Policy.

Bandwidth: The amount of data that can be moved to a computer a given period of time.

Banner Advertisement: A typically rectangular advertisement on a web site placed above, below, or on the sides of the sites main content and linked to the advertiser's own web site.

Browser: A software application used to locate and display web pages. The two most popular web browsers are Netscape™ and Microsoft Internet Explorer™. Both are graphical browsers, meaning they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins (q.v.) for some formats.

Cable Modem: A modem (q.v.) designed to operate over cable-TV lines rather than phone lines.

Cellular Wireless: A method of connection to the Internet that does not use any ground lines. The existing standard protocol is relatively slow; however, newer standards are evolving. Care must be taken to secure these networks from hackers who can literally pull information out of the air.

Central Processing Unit (CPU): The brain of the computer. Two components found in the CPU are the arithmetic logic unit, which performs calculations and logical operations, and the control unit, which decodes and executes instructions.

CPU: See Central Processing Unit.

Dial-Up Services: A dial-up service is a method of connection to the Internet through a modem and a traditional telephone line. Dial-up services are usually sufficient for using the web and e-mail applications, but are not as effective for transferring larger files (e.g., video clips).

Digital Subscriber Line (DSL): A high-bandwidth technology for connecting to the Internet using the copper telephone lines that exist in almost every home and office. Special hardware attached to both ends of the line allows data transmission at far greater speeds than standard telephone wiring and dial-up connectivity.

Domain Name: Used in URLs to identify particular web pages or sites located on the Internet. For example, the domain name *nces.ed.gov* represents the web site for the National Center for Education Statistics.

DSL: See Digital Subscriber Line.

Dumb Terminal: A dumb terminal is a "computer unit" that has a monitor and a keyboard that must connect to another computer for processing power.

File Transfer Protocol (FTP): A standard Internet protocol for transferring files from one computer to another.

Filtering: Filtering is the process of controlling access to a network by analyzing the incoming and outgoing packets. A filter lets the packets pass, or not pass, based on the IP addresses of the source and/or destination. E-mail messages and web sites can also be filtered based on content.

Firewall: An electronic boundary (or physical piece of hardware) that prevents unauthorized users and/or packets of data or information (e.g., files and programs) from accessing a protected system.

Fixed Wireless: These "computers" are wireless devices or systems that are in fixed locations, such as an office or home, as opposed to devices that are mobile, such as cell phones or personal data assistants (PDAs).

Frame Relay: A packet-switching protocol for connecting devices on a Wide Area Network (WAN). Frame relay networks in the United States support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds. Most telephone companies now provide frame relay service for customers who want connections from 56 Kbps to T-1 speeds.

Frames: A feature supported by most modern web browsers than enables the web site author to divide the browser display area into two or more sections (frames). The contents of each frame are taken from a different web page. Frames provide great flexibility in designing web pages, but many designers avoid them because current browsers support them unevenly.

FTP: See File Transfer Protocol.

Host: (n) A computer system that is accessed by a user from a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal.

(v) To host is to provide the infrastructure for a computer service. For example, a company that hosts web servers may provide the content on the server (e.g., web site or other content), but another company may control communications lines required by the server.

HTML: See Hypertext Markup Language.

Hypertext Markup Language (HTML): A formatting language used to create web pages and specify how a page will appear on screen.

Integrated Services Digital Network (ISDN): An ISDN line is a digital phone line that can transmit data, video, and voice. (ISDN lines are "point-to-point" connections from the telephone company to the computer user.)

Internet Service Provider (ISP): An ISP is an entity that provides commercial access to the Internet. Service can range in size from dial-up access with a 56-Kbps ordinary telephone line and several dozens of customers to multiple pops (i.e., connection points) in multiple cities with substantial backbones and thousands, tens of thousands, or more customers. ISPs may also provide web hosting and other services.

IP Address: An IP address is an identifier for a computer or device on a *TCP/IP* network. Networks using the TCP/IP protocol route messages according to the destination IP address. Within a private network, IP addresses can be assigned at random as long as each one is unique. However, connecting a private network to the Internet requires using publicly registered IP addresses (called Internet addresses) to avoid duplicates.

ISDN: See Integrated Services Digital Network.

Intranet: An intranet is a private, internal network that provides users access to applications within the agency.

ISP: See Internet Service Provider.

LAN: See Local Area Network.

Local Area Network (LAN): A linkage of computers and/or peripherals (e.g., printer) confined to a limited area that may consist of a room, building, or campus that allows users to communicate and share information.

List Server: A list server is a device that operates mailing lists and distributes new messages, newsletters, or other postings from list members to the entire list's subscribers. Postings can be delivered as they are received or they can be digested and delivered on a scheduled basis.

Meta Tag: A command inserted in a document that specifies how the document, or a portion of the document, should be formatted. Tags are used by all format specifications that store documents as text files.

Modem: A modem is a contraction of "modulator/demodulator." It is a device that connects the computer to a telephone line (or, perhaps, another wire) for communication with another remote computer or information network. Modems may be internal or external to the computer case. Modems are classified according to the speed with which they send and receive information.

Needs Assessment: A "needs assessment" is a process for determining the desired functions for computer and networking technology and/or determining the needs this technology will meet.

Network: A group of computers connected to each other to share computer software, data, communications, and peripheral devices. Commonly, the definition of a network includes the hardware and software needed to connect the computers together.

Node: In a discussion of networks, a "node" refers to a processing location. A node can be a computer or some other device, such as a printer. Every node has a unique network address.

Operating System: The operating system (OS) contains the electronic instructions that control the computer and run the programs. This software is generally specific to a type of computer (e.g., Windows 2000, UNIX Linux, and Mac OS X).

Packet: A packet is a message fragment containing data or information. When messages are sent on the Internet, they are broken into smaller, more easily transportable pieces called packets. Each packet consists of a header and a piece of the message. A single e-mail message may actually be broken into a half-dozen different packets.

Packet Sniffing: Packet sniffing refers to the collection and analysis of data packets (including contents) as they transit the network.

Packet Switching: Refers to the protocols within a network that determine how messages are broken into packets (q.v.) and routed to their destinations.

PDA: See Personal Data Assistant.

PDF: See Portable Document Format.

Peer-to-Peer Network (P2P): A configuration in which each computer on the network has the same capabilities as the other computers on the network and any one of them can initiate a communications session with another. Any peer can add files, copy them, and move them to any peer computer on the network (where people store their files on their own computers). Therefore, any person on the network can access those files, copy them, and move the copies over the network to another computer.

Personal Data Assistant (PDA): A PDA is a handheld device (e.g. Palm Pilot®, PocketPC®, etc.) that may combine many computing activities. PDAs that are more powerful may function as cellular phones, fax transmitters, web browsers, and personal organizers.

Plug-Ins: Plug-Ins are software pieces that add a specific feature or service to a larger system. For example, in order to view a PDF file, the Adobe Acrobat Reader® plug-in is required.

Pop-Up Ads: Advertisements that appear in a separate browser window while a web site is being viewed.

Portable Document Format (PDF): A file format developed by Adobe Systems® that captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as they were intended. To view a file in PDF format, a free copy of Adobe Acrobat Reader® can be downloaded from Adobe Systems at *www.adobe.com*.

Portal: (Also, *web portal*.) "Portal" refers to a web site or service that offers a broad array of resources and services, such as e-mail, forums, search engines, and online shopping malls. The first web portals were online services, such as AOL, which provided access to the web; now most of the traditional search engines (e.g. Yahoo®, Google®, etc.) are web portals, modified to attract and keep a larger audience.

P2P: See Peer-to-Peer Network.

RAM: See Random Access Memory.

Random Access Memory (RAM): The place in the computer where the operating system, applications programs, and data in current use are kept temporarily. When the computer is turned off, the data are removed from RAM and either stored elsewhere in the computer or deleted.

Read-Write Drive: A read-write drive is a device that enables a computer to read or write data, ranging from a simple floppy disk drive to a complex drive, which through laser technology writes data on a compact disk (CD) or a digital versatile disk (DVD).

Router: The device or software that determines the next network point to which a packet (q.v.) will be forwarded. The packet travels from point to point along the network until it arrives at its destination.

Server: A server is a computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files. Any user on the network can store files on the file server. A *print server* is a computer system that manages one or more printers, a *network server* manages network traffic, and a *database server* processes database queries. It is possible to partition the space on one computer to create more than one server.

Source Code: Source code is instructions to the computer in their original form. Initially, a programmer writes a program in a particular programming language called the source code. To execute the program, the programmer must translate the code into "machine language," the only language a computer understands. Source code is the only format readable by humans.

Spam: Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as *any* unsolicited e-mail. In addition to being a nuisance, spam also eats up a lot of network bandwidth. Because the Internet is a public network, little can be done to prevent spam, just as it is impossible to prevent junk mail. However, the use of software filters in e-mail programs can be used to remove most spam sent through e-mail.

Style Sheets: Templates for web page design that can be built into the programming of a site to provide continuity in appearance and layout across the various pages.

Surfing: To "surf" is to move from site to site on the Internet in a random or questing way while searching for topics of interest.

TCP/IP: Refers to communication protocols used to connect hosts on the Internet. TCP stands for Transmission Control Protocol, which is the main protocol in an IP (Internet Protocol) network. Whereas the IP deals solely with packet switching, TCP/IP allow two hosts to communicate with long streams of data at one time, thus always guaranteeing the packets arrive in the correct order.

Thin Client: A network computer without a hard disk drive, which, in client/server applications, is designed to be especially small so that the bulk of the data processing occurs on the server.

Universal Resource Locator (URL): A World Wide Web address composed of several parts including the protocol, the server where the "resource" (e.g., web page) resides, the path, and the file name of the resource. An example of a URL is *http://nces.ed.gov*.

URL: See Uniform Resource Locator.

W3C: See World Wide Web Consortium.

WAN: See Wide Area Network.

Web Portal: See Portal.

Wide Area Network (WAN): A data communications linkage (e.g., dedicated line, radio waves) that allows users to communicate and share information over distances greater than the distance transmitted by local area networks (e.g., building to building). The Internet is an example of a WAN.

World Wide Web Consortium (W3C): W3C is a forum for information, commerce, and collective action by a consortium of respected web inventors and developers who seek to develop technologies to enhance use of the World Wide Web *(http://www.w3.org/)*. Tim Berners-Lee, the original architect of the World Wide Web, founded W3C in 1994.

U.S. Department of Education
Institute of Education Sciences
National Center for Education Statistics
NCES 2003-381