LEGISLATIVE RESEARCH COMMISSION

PROGRAM REVIEW
AND
INVESTIGATIONS
COMMITTEE

Appropriate Management and Technology Can Reduce Costs and Risks of Computer Use by State Employees

Research Report No. 324

Prepared by

Van Knowles, Kara Daniel, Louis Pierce, and
Greg Hager, Ph.D., Committee Staff Administrator

Appropriate Management and Technology Can Reduce Costs and Risks of Computer Use by State Employees

Program Review and Investigations Committee

Greg Hager, Ph.D.
Committee Staff Administrator

Project Staff

Van Knowles
Kara Daniel
Louis Pierce

Research Report No. 324

Legislative Research Commission
Frankfort, Kentucky
lrc.ky.gov

Adopted September 9, 2004

Paid for with state funds. Available in alternative form by request.

Foreword

For their cooperation with this study, Program Review and Investigations Committee staff would like to thank Secretary Robbie Rudolph, Kristen Webb, and the staff of the Finance and Administration Cabinet, especially Commissioner Mike Inman, Mark Rutledge, Scott Render, and Dodd Harris of the Commonwealth Office of Technology; Howard Lawson, Carl Felix, and Neal Lanham of the Personnel Cabinet; Don Pendleton and Kevin Rader of the Department of Criminal Justice Training; and James Ramsey, Shawn Estep, and Rob Elliott of the Transportation Cabinet.

Personnel too numerous to mention from the following agencies provided helpful responses to the inquiries of Program Review and Investigations Committee staff: Commerce Cabinet, Department of Corrections, Cabinet for Economic Development, Education Cabinet, Cabinet for Health and Family Services, Justice and Public Safety Cabinet, Department of Juvenile Justice, Department for Libraries and Archives, Department of Military Affairs, and Department of Veterans Affairs.

The staff of the Program Review and Investigations Committee would like to extend special acknowledgment to Ashland, Inc.; SAS Institute, Inc.; United Parcel Service, Inc.; Anne Lovell of the Tennessee Office for Information Resources; and Elayne Starkey of the Delaware Department of Technology and Information for providing background information about their approaches to managing acceptable computer use. Chris Dixon of the National Association of State Chief Information Officers was very helpful in locating information from other states.

Robert Sherman
Director

Frankfort, Kentucky
September 9, 2004

Contents

List of Tables

List of Figures

Summary

Awareness of the issue of computer misuse increased in 2003 due to a widely reported scandal involving access to pornographic Web sites by some Transportation Cabinet employees. Fortunately, such headline-worthy abuse is rare. But even routine computer misuse by Kentucky state government employees can impose significant real or potential costs such as lost productivity, extra costs for computer resources, increased legal liability, and increased computer security risk. The same statement would be true about many other organizations. Computer misuse has been documented in other state governments, federal agencies, local governments, universities, and private companies.

Over the past year, Kentucky has taken great strides in recognizing problems related to computer misuse and implementing solutions. A task force has been created with the objective of drafting a regulation that will give the state's acceptable use policy the force of law. Awareness of and compliance with the policy will be a part of employee evaluations. The Commonwealth Office of Technology is implementing a system to block access to inappropriate Web sites and make it easier for executive branch agencies to manage computer use more efficiently and effectively. Many agencies now are making acceptable computer use a higher priority. No system can be perfect, but improved management and use of technology should make a repeat of the 2003 scandal much more difficult.

On December 17, 2003, the Program Review and Investigations Committee authorized a study of inappropriate computer use by state employees. In conducting the study, staff conducted interviews and gathered computer use management information from major executive branch agencies, other states, federal agencies, educational institutions, and private companies. Staff reviewed other research on this topic and did legal research to determine risks and best practices.

The major conclusions below serve as a brief summary of the main points of this study. In general, state government has made significant progress in preventing computer misuse. Following the conclusions are this report's specific recommendations to improve current policy and procedures.

Major Conclusions

Besides loss of goodwill or adverse publicity, the primary areas of cost management are employee productivity (job performance), costs of equipment and services, legal liability, and the risk of cyber attacks on state computing systems. The way employees use computers bears directly on each of these costs. Most of these costs and risks are the same as those associated with other employee behavior or the use of other state government equipment and services. Management of acceptable computer use, therefore, requires good employee supervision and relations, as well as information technology tools. Cost avoidance from good management of acceptable computer use could range into the millions of dollars.

Some Kentucky agencies have done an excellent job managing computer use; others have not done as well. The new centralized strategy for managing statewide computer use should be fully implemented by September 30, 2004, and appears very promising for a number of reasons. It has commitment from the Governor's Office, Personnel Cabinet, Finance and Administration Cabinet, and Commonwealth Office of Technology. It utilizes state-of-the-art technology to block inappropriate access to the Internet and to monitor e-mail. The technology operates without action by individual agencies, yet it allows agencies to add stricter controls. The strategy includes procedures to inform and remind employees about the policy. With the issuance of an administrative regulation, it will carry the force of law.

Program Review staff found some aspects of Kentucky's acceptable use policy and procedures that could be improved, but the basic approach is thorough and sound. The greatest challenge will be motivating management and employees in all agencies to incorporate acceptable use into their workplace culture.

A remaining issue is how we will know if the new controls are working. The Commonwealth Office of Technology and Personnel Cabinet lack the ability to measure the effectiveness of acceptable use policies and procedures. An oversight office or council is needed to ensure that the acceptable use policy and procedures are effective, up-to-date, and of high priority.

The following are summaries of each of the 11 detailed recommendations found in the report. The full text of each recommendation can be found in Chapter 3.

Recommendations

Recommendation 3.1

The acceptable use task force should consider making specific additions or improvements to the Internet and e-mail acceptable use policy and all related policies.

Recommendation 3.2

The acceptable use task force should review the applicability of acceptable use policies to all possible users of executive branch computer resources.

Recommendation 3.3

The Personnel Cabinet and the human resource staff of each agency should implement an ongoing process to establish and promote a corporate culture of proper use of the Commonwealth's computer resources.

Recommendation 3.4

The Personnel Cabinet should assure that the Kentucky Employee Handbook section related to use of information technology resources is always as accurate and understandable as possible.

Recommendation 3.5

The Commonwealth Office of Technology and the information technology office of each agency should consider taking specific actions to manage file storage, local network capacity, and workstation security.

Recommendation 3.6

The Finance and Administration Cabinet should consider allowing access to non-work-related Internet sites that are appropriate for personal use subject to supervision at the agency level.

Recommendation 3.7

The Personnel Cabinet should design outcome measures for all agencies to determine the effectiveness of acceptable use management on employee knowledge and behavior, including employee knowledge and support of the policies and incidents of inappropriate use and their disposition.

Recommendation 3.8

In addition to bandwidth use, the Commonwealth Office of Technology should retain adequate information about Web access and e-mail use to track important factors over time.

Recommendation 3.9

The Commonwealth Office of Technology should increase its testing of computer system security.

Recommendation 3.10

The Personnel Cabinet and the Finance and Administration Cabinet should review acceptable use policies and procedures at least annually.

Recommendation 3.11

The Personnel Cabinet, Finance and Administration Cabinet, and Office of the Governor should formalize the acceptable use task force as a permanent entity with responsibility to review all policies and procedures related to acceptable computer use on a regular basis, oversee their management, and communicate their status to the governor and to executives in all agencies.

Glossary of Computer Terms

adware: Software programs that secretly gather information about the user's identity and Internet browsing habits and relay the information to an advertising or marketing company. Adware is usually installed without the user's knowledge while Web browsing or reading e-mail or other forms of electronic messages.

antivirus: A general term applied to software programs and hardware that detect and protect against other harmful software programs, such as viruses, worms, and Trojan horses.

bandwidth: A measure of how much information can be carried on a given network connection at one time, typically given in number of bits per second.

bit, byte, kilobyte, megabyte, gigabyte: A bit is the smallest piece of information that can be represented. It is a yes/no indicator, consisting of a 1 or 0. A byte is a sequence of 8 bits. A kilobyte is approximately 1,000 bytes, a megabyte equals approximately 1 million bytes, and a gigabyte is approximately 1 billion bytes.

chat: In Internet terminology, a form of instant messaging among groups of individuals.

Chief Information Officer: typically an executive with responsibility for managing information technology staff and resources in an organization.

content security management (CSM): This refers to a software product, sometimes combined with hardware, that performs several functions related to computer system security. What distinguishes a CSM from other products is its ability to control the content of Internet browsing and e-mail messages by, for example, blocking access to certain types of sites or intercepting e-mail that contains offensive phrases.

cyber attack: Any of a number of ways that outsiders can attempt unauthorized access and/or damage to a computer system.

domain: An Internet term that refers to a category or type of Web site. Common domains are .com, .edu, .org, .gov. The domain is the rightmost part of an Internet site address.

encrypt: To convert information into a form that cannot be read by anyone who does not have a secret "key." Encryption is usually used to protect sensitive information when it is transmitted over a public network, such as e-mail or the Internet, or when it is stored on a computer system of any kind.

file server: A computer that sits between the user and file storage devices on a network. The file server receives requests to store or retrieve data, determines whether the request is valid, and if so, handles the request.

firewall: (1) A hardware device that sits between a local network or workstation and the Internet or between two systems in general that protects one of the systems from certain kinds of unauthorized access.
(2) A software program, running on a server or workstation, that protects the computer from certain kinds of unauthorized network or Internet access.

hacker: An unauthorized person who uses software tools, such as worms and Trojan horses, to observe, obtain information from, gain control over, and/or damage computer systems.

instant messaging: Any of a number of methods for exchanging messages immediately and conversationally between users on a network or the Internet.

peer-to-peer (P2P): A method of sharing files over the Internet or other networks without using traditional file or Web servers.

proxy server: A computer that sits between the user and the Internet. This computer intercepts all user requests for Internet access. It can perform a number of functions: caching (keeping a copy of frequently used Web pages so that they do not have to be retrieved from the Internet every time), blocking (preventing access to certain sites or certain methods to access sites), security, and monitoring.

server: A computer that provides services to multiple users, typically over a network.

social engineering: A method of cyber attack in which a hacker attempts to trick computer users into providing access to computer systems. For example, a hacker could impersonate an information technology security officer and request a user's password. An e-mail that asks a user to open an attachment containing a virus is a form of social engineering attack.

spam: Unsolicited electronic messages, typically e-mail, usually attempting to sell a product or service. Often these are disguised as business or personal messages.

spyware: Software programs secretly installed on a computer that gather sensitive information (such as passwords) or capture everything typed on the computer and send the information to someone (typically a hacker) without the user's knowledge.

Trojan horse: A software program that can take control of some computer functions in order to disable system security, send messages to its originator, or damage data. Trojan horses do not replicate themselves but typically are intended to provide an opening for a hacker to obtain information about or control of a computer.

virus: A software program that can take control of some computer functions in order to reproduce itself by attaching itself to other software programs. Sometimes viruses perform other actions, such as displaying messages or destroying data. Most viruses do not destroy data.

Web server: A computer that contains a Web site and receives requests to view Web pages. It will return the requested page if the user is authorized.

workstation: An individual personal computer with a single computing unit, intended for use by one person at a time.

worm: A software program that can take control of some computer functions in order to copy itself to other computers via local networks, e-mail, or other means. Sometimes worms perform other actions, such as disabling system security or destroying data.

Source: Compiled by Program Review Staff from Symantec® Security Response glossary and Wikipedia™ online encyclopedia.

Chapter 1

Inappropriate Computer Use and Its Costs

Introduction

Computers, e-mail, and the Internet help government employees provide services more quickly and effectively. For many state workers, these are indispensable tools used daily. However, the qualities that make computer tools so useful, such as speed and access to a worldwide information network, can also lead to misuse.

The Transportation Cabinet disciplined 46 employees for using work computers to access pornography.

For example, in 2003 the Kentucky Auditor of Public Accounts discovered that hackers, probably from another country, had broken into a state proxy server and built a library of pirated movies, textbooks, DVDs, and CDs. The Auditor also documented that more than 200 computers assigned to Transportation Cabinet employees had been used to access pornographic Internet sites (Loftus). A follow-up investigation by the Transportation Cabinet's Inspector General found that, although some of the suspected sites were not pornographic, there was enough evidence to discipline 46 employees for inappropriate use (Elliott).

Computer misuse has become a serious problem in many organizations.

Given that the Transportation Cabinet was not deliberately selected for this type of monitoring, it is possible that similar inappropriate use was occurring in other state agencies as well. The Commonwealth Office of Technology (COT) has provided some overall evidence of this misuse and estimated that lost productivity alone could cost Kentucky millions of dollars per year (Commonwealth of Kentucky. Governor's Office for Technology). Kentucky is not alone. Computer misuse has been documented in state governments, local governments, universities, and private companies.

Kentucky has made major improvements in managing acceptable use.

Over the past year, Kentucky has taken great strides in recognizing the problem and implementing solutions. A task force has been created with the objectives of drafting a regulation that will give the policy on acceptable computer use the force of law, including awareness of and compliance with the policy as part of employee evaluations, and fostering employee awareness. COT is implementing a system, scheduled to be in place by September 30, 2004, to block access to inappropriate Web sites. Many agencies now are making acceptable computer use a higher priority.

Description of This Study

How This Study Was Conducted

For this report, staff examined policies and procedures, reviewed best practices, and researched legal risks.

On December 17, 2003, the Program Review and Investigations Committee authorized a study of inappropriate computer use by state employees. In conducting the study, staff interviewed officials with COT, the Personnel Cabinet, and other executive agencies. Staff obtained information on executive branch agencies' human resource and information technology practices in managing computer use.

For comparison, staff obtained acceptable use policies and/or interviewed officials from a total of 24 other states, federal agencies, educational institutions, and industry. Staff also reviewed model policies, other studies, and research on managing computer use. Finally, staff conducted legal research on liability issues related to the use of computers.

Organization of the Report

The remainder of Chapter 1 summarizes basic approaches to managing computer use, and describes the real and potential costs for categories of computer use. Chapter 2 reviews best practices in the development and implementation of acceptable use policies. Chapter 3 assesses Kentucky's previous and current management of acceptable use.

Appendix A briefly discusses related issues that may merit further consideration but that are beyond the scope of this study. Appendix B provides more details on the research methods used for this report. Appendix C contains documents relevant to the state acceptable use policy. Appendix D is the Finance and Adminstration's response to this report. Appendix E is the Personnel Cabinet's response.

Major Conclusions

Staff reached five major conclusions:
1. The risks associated with computer use by state employees are varied and significant.

1. Risk associated with computer use by state employees can be classified as

- loss of goodwill through adverse publicity,
- lost productivity,
- equipment and services above those needed to serve business needs,
- lawsuits against the Commonwealth, and
- data loss and needed system recovery due to cyber attacks.

Savings from good management of acceptable computer use could range into the millions of dollars.

2. Effective management of employees in general should reduce inappropriate computer use.

2. Most of the risks are not caused by computer use itself. For example, harassing coworkers and wasting time occurred before the advent of computers. Further, all computer use involves risks, whether it is work-related or not. Management of acceptable computer use requires good employee supervision and relations, commitment from the top, and effective use of information technology tools.

3. The new centralized strategy for managing computer use looks promising.

3. Some Kentucky agencies have done an excellent job managing computer use; others have not done as well. The new centralized strategy for managing statewide computer use appears promising because it

- has commitment from the highest level;
- uses state-of-the-art technology to block inappropriate access to the Internet and to monitor e-mail;
- uses technology that operates without action by individual agencies, yet allows agencies to add stricter controls;
- includes procedures to inform and remind employees about the policy; and
- will carry the force of law through an administrative regulation.

4. Management and employees must be motivated to incorporate acceptable computer use into workplace culture.

4. Some aspects of Kentucky's acceptable use policy and procedures could be improved, but the basic approach is thorough and sound. The greatest challenge will be motivating management and employees in all agencies to incorporate acceptable use into their workplace culture.

5. The Commonwealth Office of Technology (COT) and the Personnel Cabinet lack the ability to measure the effectiveness of acceptable use policies and procedures.

5. The Commonwealth Office of Technology and the Personnel Cabinet lack the ability to measure the effectiveness of acceptable use policies and procedures. An oversight office or council is needed to ensure that acceptable use policy and procedures are effective, up-to-date, and of high priority.

Acceptable Use Is Accomplished by Managing Employee Behavior and Computer Systems

Policies should be well-written and implemented appropriately.

This report will focus on ways to ensure acceptable use of state government's computer resources. Management of this issue, as with any business issue, requires first that clear, comprehensive, and enforceable policy be written.

Human resource and information technology approaches are both necessary to implement acceptable use policy. Human resource methods involve employee accountability and involvement. Information technology methods monitor or restrict what employees do with computer systems.

Once policies have been written, the procedures to carry them out must be created. There are two basic approaches: human resource (also referred to as personnel or management) and information technology. It cannot be stressed enough that successful management of employees' use of computers will usually require elements of both approaches. Human resource (HR) methods entail employee accountability and involvement. Information technology (IT) methods monitor or restrict what employees do with computer systems. Educating employees about appropriate computer use and making computer use part of performance evaluation are examples from the HR approach. Blocking access to Internet sites deemed inappropriate by management is an IT method. Table 1.1 lists a number of approaches from each.

Table 1.1
Approaches To Managing Acceptable Use

Human Resource	Information Technology
• Workload management	• Monitoring tools
• Employee accountability	• Filtering (blocking) tools
• Employee education / training	• Investigative tools
• Employee motivation	• Security (protective) systems
• Disciplinary action	

Source: Compiled by Program Review staff.

Human Resource Procedures

Management has responsibility for creating the environment in which employees will behave appropriately, but employees are also accountable for their behavior. Human resource policy should include procedures to inform employees of the acceptable use policy and to verify that employees were informed. Good HR practice also includes education in acceptable use and system security practices, frequent reminders, feedback from and to employees, complaint and investigation procedures, and a disciplinary process.

Information Technology Procedures

Information technology can make it harder for employees to misuse computer systems and easier for employers to detect and correct such behavior. Software tools exist to record employee activity and to filter or block access to inappropriate information and messages. Additional tools can be applied when investigating specific allegations. Security features, from password enforcement to firewalls and antivirus software, protect systems from unauthorized access and cyber attack.

Acceptable Versus Inappropriate Use

Inappropriate use is anything that is not acceptable use.

Although inappropriate computer use has received much attention, most computer use is proper and necessary to carry out the business of the Commonwealth. Most policies on this topic include "acceptable use" in their titles and encourage employees to take full advantage of computers to provide better service. Once acceptable use is understood, inappropriate use is everything else.

For the purposes of this study, "acceptable use" is defined as

- any use of computer resources for legitimate business purposes, conducted in a safe and secure manner; and
- incidental (personal) use, if permitted.

Acceptable use can include incidental (personal) use.

Typically, incidental use must have little or no cost to the employer, must occur on personal time, and must be safe, legal, and ethical. Examples of incidental use include allowing an employee to e-mail her daughter or use the Internet to check her credit union account. This is similar to allowing employees some personal telephone calls. Incidental use was allowed by 78 percent of the policies of states, federal agencies, and other organizations reviewed by Program Review staff. Kentucky's current policy includes incidental use.

In one sense, a computer is similar to other office equipment in that it can be used productively or not. The same pen that can be used to write memos can be used to work a crossword puzzle when the employee should be working. The same computer can be used to write memos or work crossword puzzles online.

Computers are different, however, in the breadth of tasks—appropriate or inappropriate—that they can be used to accomplish. As there are many ways to use computers productively, there are many ways to misuse them—sometimes at high cost. Table 1.2 shows several of the tasks that computers can perform, along with business and personal uses for each. Some of the personal uses are clearly inappropriate, but many could be included in acceptable incidental use as determined by management.

Table 1.2
Business Versus Personal Uses of Computer Systems

Business Function	Business Uses	Personal Uses
Storing Information	Storing and retrieving business information	Storing and retrieving personal or illegal information
Printing	Producing business documents	Producing personal documents
Reproducing information	Archiving business data and software	Making unauthorized copies of business information, software, music, or videos
Multimedia presentations and interactive media	Work-related broadcasts, meetings, or workshops; interactive training; video conferencing	Listening to music or watching videos; playing computer or Internet games
Accounting	Tracking operational expenses	Tracking personal expenses
Providing information to the public	Business Web sites	Personal Web sites
Accessing public information	Business-related research	Personal browsing
Sending messages	Internal and external business communication	Personal messages
Linking remote business units and users	Sharing internal information, customer support, remote system management	Unauthorized access to other systems, permitting unauthorized access to user's system

Source: Compiled by Program Review staff.

Costs of Improper Computer Use

Computer use, especially inappropriate use, creates financial and legal risks.

Inappropriate use of computers by employees can create significant real and potential costs. Even legitimate business use can have costs. The remainder of this chapter addresses these issues. Table 1.3 provides an overview.

Table 1.3
Major Costs of Improper Computer Use

Cost	Description
Lost goodwill	• Adverse publicity due to egregious misuse of computer systems • Adverse publicity due to exposure of confidential information
Lost productivity	• Use of computer systems that interferes with job performance of self or others
Capacity costs	• Purchase of equipment or services beyond those needed strictly for business purposes
Damage to systems and data	• Failure to follow best practices, leading to cyber attack from the outside • Collusion with cyber attack or intentional damage by an employee
Legal liability	• Civil awards if employee use results in economic damages or violation of protected rights • Civil awards if employer action to enforce policy is found to be unfairly applied or an invasion of privacy • Civil contempt if record retention policies are not followed

Source: Compiled by Program Review staff.

Inappropriate Use Can Lead to Loss of Goodwill

Goodwill is an intangible resource, but its loss can have devastating effects.

Although it is very difficult to measure, lost goodwill is a real cost when improper computer use by an agency's employees becomes public knowledge. Adverse publicity can harm not only the reputation of the agency and its officials but also that of state government and its employees in general. For example, over the past two years, there were more than 25 articles in four major state newspapers on the Transportation Cabinet's computer pornography scandal.[1] National media also picked up the story. It would be hard to argue that the state's image was helped by the following headlines:

- In Brief/Kentucky: "State Computers Seized in Child Porn Inquiry" (*Los Angeles Times*, August 9, 2003);
- "Agency Computers Seized in Porn Probe," Dateline: Frankfort, Kentucky (*Chicago Tribune*, August 10, 2003); and
- "Kentucky State Computers Used to View Porn" (*Miami Herald*, May 29, 2004).

The potential for adverse publicity is not limited to Internet use or to Kentucky state government. For example, tasteless e-mail messages may be forwarded to many recipients to whom the sender may or may not have intended, or an inappropriate

[1] The newspapers searched (and the number of articles found) were the *Kentucky Post* (7*), Lexington Herald-Leader* (7*),* Louisville *Courier-Journal* (9) and Owensboro *Messenger-Inquirer* (3).

employee-to-employee e-mail may lead to a lawsuit. Even if misuse is localized, records may remain on hard drives and servers after being deleted by the employee. These records are accessible to those involved in criminal proceedings, civil proceedings, or, in the case of state government, open records requests.

Washington state's Department of Labor and Industry was beset by scandal in 2001 and 2002. Over that period, 8 employees were terminated, one resigned, and 11 received penalties for excessive personal use of e-mail (Parvaz). The investigation stemmed from a sexual harassment suit and quickly ballooned into a public relations nightmare. The *Seattle Times* dubbed the agency the "Department of Lust and Indecency" (Thomas and Garber).

In August 2004, the British public learned of the results of eight months of monitoring of the Department of Work and Pensions. More than 200 employees were disciplined for downloading pornography at work (BBC News).

Inappropriate Use Can Lead to Loss of Productivity

Lost productivity could well be the greatest financial cost associated with improper computer use. If employees are using computers for personal activity on work time, they are not doing their jobs. Such usage also ties up computer resources and can affect the productivity of other employees, by slowing e-mail and network access, for example.

It should be stressed, however, that reducing or eliminating improper computer use does not automatically make employees more productive. Employees might use computers for nonwork purposes on work time after their assigned work tasks are completed. Employees might also use computers for personal purposes instead of doing their work. In either case, eliminating personal computer use would lead to increased productivity only if employees did more useful work than before. If time that was spent on personal computing is now devoted to other nonwork activities, then productivity will not increase (Solomon).

It is possible that a computer use policy itself can lead to a loss in productivity. Depending on how the policy is implemented, some employees may seek other employment (Urbaczewski and Jessup). Replacing employees takes time and there is no guarantee that the replacements will be more productive. Disgruntled employees who

stay may be less motivated to give extra effort as needed or to create solutions to workplace problems (Moorman and Wells).

Internet

It is likely that lost productivity due to personal use of computers is significant. COT estimated lost productivity at $168 million per year. Based on a different survey, Program Review staff estimated lost productivity at $77 million per year.

In 2003, COT estimated the value in lost productivity due to personal use of the Internet by Kentucky state employees was $168 million per year. This estimate was based on 35,000 employees spending one hour per day on "nonproductive surfing" at $20 per hour for 240 workdays. This was given as a "conservative cost," based on an industry survey showing that on average employees spend one to two unproductive hours surfing per day (5 to 10 hours per week) (Commonwealth of Kentucky. Governor's Office of Technology).

It should be kept in mind that this is just one estimate of the financial value of lost productivity. Due to a lack of reliable data, estimates vary greatly. For example, Program Review staff calculated an estimate of $77 million per year based on a survey conducted in early 2004 (Websense, "Web@Work").[2] Either $168 million or $77 million or some number in between represents valuable time that should be converted to productive work. Eliminating unproductive employee time seems unlikely, but a combination of HR and IT strategies could result in a significant reduction.

E-mail and Other Messaging

Use of e-mail at work has expanded, but few surveyed employees reported large numbers of personal messages.

Between 2000 and 2002, the number of U.S. workers using e-mail grew from less than 30 million to more than 57 million (Fallows 5). A precise measure of the time employees spend on personal e-mail is unknown. One survey found that for about 90 percent of employees, personal e-mail comprised 10 percent or less of their messages. For about 3 percent of employees, personal e-mail accounted for over 25 percent of their messages (American Management Association 7).

Other forms of Internet messaging are available. "Chat" and "instant messaging" allow real-time written communication between two or more computer users. Peer-to-peer file sharing

[2] Of employees surveyed, 86 percent said they use the Internet at work. Of these, 59 percent said they sometimes used it for personal surfing on work time, which accounted for 51 percent of all employees. Their reported personal surfing time averaged about three hours per week. IT managers estimated these employees spent about six hours per week. The estimate of $77 million was reached by splitting the difference between the estimates of employees and management to get 4.5 hours per week applied to 51 percent of employees.

allows computer users to share the contents of storage devices, such as hard drives. Peer-to-peer file sharing has been used primarily as a way of sharing audio and video files.

Not many employees report a problem with spam, but the problem is growing.

The other productivity cost associated with e-mail is spam. A recent survey reported that this is a significant issue for 2 percent of workers (American Management Association 5), supporting an earlier survey that indicated spam was not a problem for most workers (Fallows 10). Program Review staff were unable to determine whether this was due to proper employee use of work e-mail or to spam-blocking software.

In general, research suggests that the volume of spam is growing, and employees are primarily innocent victims. Employees may not read their spam thoroughly, but they still have to spend work time sorting out which messages are spam and which are not. Reducing or eliminating spam would appear to be an effective way to improve productivity.

Workstation Use

A computer workstation by itself offers ways to waste time, such as playing games or listening to CDs.

Web surfing and e-mail are not the only sources of lost productivity, but they have gotten the most attention. Some employees use their workstations to play games, such as solitaire. The computer can also be used to write personal letters, keep personal spreadsheets, and play music CDs or even movies. Program Review staff did not find much reliable research on this issue. Workstation monitoring does not appear to be common for professional and administrative employees, and surveys have not asked about workstation use.

Inappropriate Use Can Lead to Unnecessary Purchases of Equipment and Services

Another financial cost is system capacity. System traffic jams caused by excessive personal use, as well as use of data storage space for personal files, can result in state government's paying for more computer resources than would be necessary if all use were work related.

Internet Bandwidth

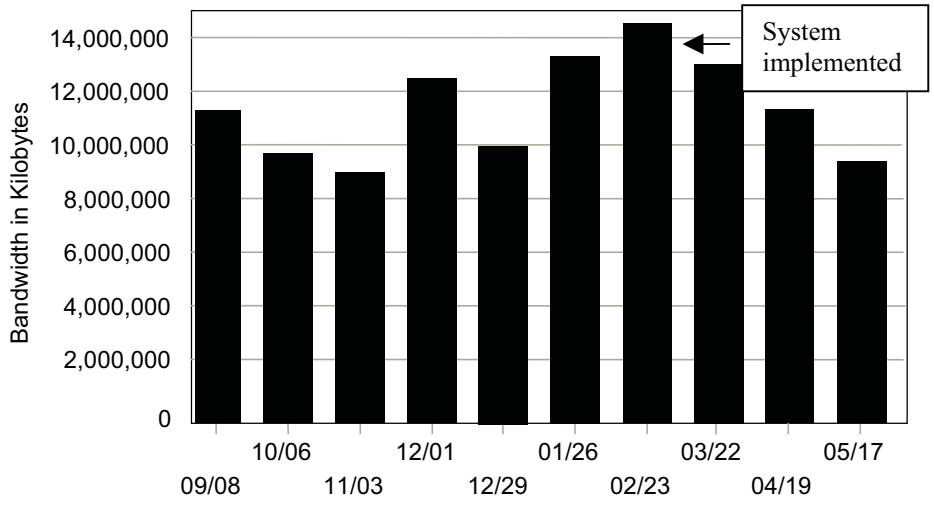
The Kentucky Information Highway has had occasional outages because demand has exceeded capacity.

A major concern of COT is the rapidly increasing demand for Internet bandwidth—the amount of information that an Internet connection can carry. The Kentucky Information Highway is the statewide Internet access pipeline for state government and many other users. In February 2002, the bandwidth for the Kentucky Information Highway was increased from 90Mbps (megabits per second) to 155Mbps. It remained at that capacity until late June 2004. Mark Rutledge, executive director of COT's Office of Infrastructure Services, told staff that demand had exceeded this capacity several times, leading to temporary Internet outages. A recent increase in capacity to 200Mbps resulted from the needs of public schools and other users of the Kentucky Information Highway outside state government.

Kentucky is implementing a system that might result in a 20 to 50 percent reduction of demand for bandwidth.

Faced with the likely expense of adding capacity, COT conducted a pilot program in which Internet access to particular Web sites was blocked. During the pilot, demand for bandwidth decreased significantly. The Personnel Cabinet implemented the same system with similar results. Between February and May 2004, Personnel's Internet bandwidth use declined by 35 percent, as shown in Figure 1.A. Estimates of potential reduction of bandwidth use for the Commonwealth range from 20 to 50 percent.

Figure 1.A
Personnel Cabinet's Internet Bandwidth Use
Sept. 2003 to May 2004



Source: Productivity Report from Personnel Cabinet, System Management Branch, July 6, 2004. Modified by Program Review staff to remove incomplete data for June 2004.

Personal browsing has led the state to purchase significantly more Internet bandwidth than needed strictly for its business.

This does not necessarily mean that state employees are spending 20 to 50 percent of their Internet time on inappropriate sites. It probably means that personal browsing typically leads to Web pages that use more bandwidth than work-related pages. However, it does mean that the amount of incidental Internet use by state employees has led to the purchase of more capacity than would have been necessary for strictly work-related purposes. COT has estimated that the cost avoidance in this area alone will nearly offset the cost of the blocking system.

In the same way that the Internet gateway has limited capacity, the local networks that connect individual workstations to the Internet have an upper limit on bandwidth. Besides providing the Internet connection, local networks provide common computer file storage via file servers. The transfer of files over the network also consumes bandwidth.

To the extent that personal use of the Internet, e-mail, and network file access pushes the limits of these local networks, agencies are faced with increased costs. Higher-capacity wires are required sooner than they otherwise would be. Estimates of cost ranged from $100 to $200 per workstation to upgrade network wires. However, Program Review staff were unable to estimate how often such wires would have to be upgraded in the normal course of business, or how much sooner an upgrade might be required because of personal computer use.

File Storage

Program Review staff examined the issue of whether personal files, such as MP3 music files, video clips, game software, and other nonbusiness files created a shortage of file storage space. Because such personal files are many times larger than a typical word processing document or spreadsheet, this seemed to be a likely cost risk.

The cost of file storage space for personal files does not appear to be a major cost risk.

Staff found very little published information on this subject. Many companies have concerns about employee use but are handling it with quotas on how much storage space each user may occupy (Ferrarini). Staff found that some organizations scan their file servers for unusually large files and remove them if they are not business related. Some organizations also prevent any unauthorized software from being installed on workstations. Personal files might be stored on local workstation drives at no extra cost to the employer. Today, the typical new workstation will include at least 20 gigabytes of storage. The relatively low cost of

storage, the use of storage quotas, and the ease with which system administrators can identify unusually large files probably mitigate much of the risk.

Computer Systems and Data Can Be Damaged

Damage to computer systems and data can occur whether the use was appropriate or not.

In the course of legitimate or inappropriate activity, all computer use carries the risk of cyber attack. Computer worms, viruses, Trojan horses, and direct scans by hackers bombard all computer networks. Even an isolated computer workstation can become infected. Such an infection could result in lost work files, the financial costs of recovery, and confidential information being exposed to outside parties.

Employees contribute to the risk of cyber attack when they fail to understand and follow best practices for computer security. Employees can also assist a cyber attack or damage systems intentionally. Both accidental and intentional damage can be seen as forms of inappropriate computer use.

Cyber attacks can create losses on a number of fronts. Spying to obtain sensitive or confidential information is a legal risk. This and other types of attack, such as Web site defacement, also result in adverse publicity. At a minimum, any attack will require IT resources to remove the infection and will result in some lost productivity.

While cyber attacks can result in other kinds of loss, the most serious is to the data and computers themselves.

Sometimes a cyber attack will result in sabotage—deliberately erasing data or destroying system software. It is possible to create remote software agents that can damage computer hardware. The costs involved include the IT staff's time for system recovery, replacement of damaged computers, productivity lost while workers cannot use their computers, and the expense of reconstructing any lost data that was not backed up (Weaver and Paxson 2, 7).

Uninformed or careless employees can inadvertently facilitate a cyber attack.

IT security tools are the first lines of defense against cyber attacks; however, appropriate use by employees, especially careful Internet and e-mail use, can reduce the chances of a successful and expensive attack. An uninformed, careless, or inappropriate user can open the door to hackers and the damage they can inflict. One survey reported that 11 percent of the "worst" attacks were caused by inappropriate use (Loney). A survey of employees in the United Kingdom showed that about 90 percent felt "they have no part to play in protecting their machines" and "two-thirds admitted to

having no knowledge of basic virus-prevention measures" (Bennett).

Unfortunately, there are nearly 68,000 known computer viruses, and a single virus can result in significant costs.[3] The Commonwealth of Virginia had its computer security compromised by the ILOVEYOU computer virus in 2000. The virus spread through e-mail, sending itself to everyone on the recipients' e-mail lists. Fifty-seven of 100 agencies reported the virus had infected their hardware; another 14 reported that their hardware was affected but not infected. Agencies affected by the virus estimated a total cost of over $645,000 due to lost productivity, staff hours devoted to recovery, and hardware and software costs (Commonwealth of Virginia).

In Kentucky, COT has reported eight computer virus outbreaks since the beginning of 2003. Based on industry guidelines, COT estimated that state agencies spent approximately $1.6 million to recover from these attacks, or about $85,000 per month during 2003 and 2004. This does not include the cost of protective measures purchased and operated by the state, such as firewalls and spam e-mail filters.

Computers Increase Exposure to Legal Liability

An employer may bear some legal responsibility for employee behavior and face limits on personnel actions and records management.

Some employees' behavior may violate someone's rights or cause other damages. For instance, if an employee hangs an obscene photo on his or her wall, a coworker may consider this a form of sexual harassment. As another example, if an employee has access to information about a proprietary industrial process and accidentally places that information in a letter to a competitor, the owner of the process may claim economic damages.

With computers, employees have more opportunities to violate rights and cause damages. The Internet's broad reach can bring offensive material to the employee's fingertips. Intellectual property—copyrighted music, videos, articles, and software—is instantly available. E-mail provides an easy means to exchange harassing, offensive, or defamatory messages. Word processing programs make it easy to copy others' work and claim it as one's own. The Internet, e-mail, and office software also increase the likelihood of mistakes, such as sending information to the wrong person or issuing a draft document before it is approved. Computer

[3] According to the Symantec® Norton Antivirus® software program, there were 67,994 viruses as of August 25, 2004.

use requires vigilant awareness and care to ensure that all legal rights and property are protected.

The State Can Be Liable for Employees' Actions

The term "employee" needs to be understood to include anyone working at the behest of the employer, including contract workers, interns, and volunteers.

State government can be held legally liable for the actions of its employees, subject to sovereign immunity.

The state, like all employers, can be held legally liable for the actions of its employees under the doctrine of "vicarious liability." Thus, if an employee misuses an office computer in a manner that causes harm to another individual, the state can be held liable for the resulting damage. The employee would have to commit the act "in the scope of employment," meaning in a manner somehow facilitated by or connected to the authority of his or her position. This standard is broad enough to encompass many illegal acts committed in the workplace. Vicarious liability only applies to monetary damages not to criminal penalties.

The state may also be subject to liability for its employees' actions under traditional negligence standards. If the employer is deemed to have a duty to protect third parties from its employees' actions due to its ability to control or monitor those actions, and if it fails to do so, then the employer can be held liable to the third party for the resulting damage (Mooney). This standard is much harder to meet since courts disfavor imposing such duties on employers, but it is a possibility that should be noted, and which could apply to computer misuse.

The state's liability is limited by the doctrine of sovereign immunity under common law and the 11th amendment of the U.S. Constitution. This doctrine provides that the state cannot be sued for damages, under state or federal law, unless it expressly waives its immunity or a federal law specifically provides for damages. However, Kentucky has waived its immunity by creating the Board of Claims in KRS 44.070. Under the provisions of this and related statutes, liability is limited to $200,000 for a single claim and $350,000 for multiple claims arising from a single incident. It is also limited to actual damages and excludes damages for emotional pain and suffering. Finally, if a specific federal law provides for damages pursuant to the 14th amendment, liability might not be limited.

With these parameters in mind, the state's liability for employee computer misuse is most likely to arise in the following situations.

If employees use computer resources to harass or discriminate against individuals on the basis of race, sex, or other protected classifications, the state could be liable for creating a hostile work environment.

Sexual Harassment and Hostile Workplace. If employees, especially those in supervisory positions, use computer resources to harass or discriminate against individuals on the basis of race, sex, or other protected classification, the state could be liable for creating a hostile work environment. This is particularly true in the case of sexual harassment, which can occur if pornography or sexually explicit materials are viewed, downloaded, or distributed in the workplace, or through the use of harassing e-mail messages.

Employers can be vicariously liable for harassment creating a hostile work environment. Although it is also illegal under state law, sexual harassment actions are usually brought as federal claims under Title VII of the Civil Rights Act. Under this act, the state could be subjected to unlimited liability from sexual harassment claims if computers are misused in this manner. Damage awards and settlements in such cases have exceeded $1 million (ABC News; Chiang).

Copyright Infringement. Copyright law is complicated, but infringement occurs when an individual reproduces, distributes, or otherwise uses copyrighted material without permission and without qualifying as a recognized exception. Unauthorized use can include electronic downloading, distributing, and file sharing of copyrighted computer software, music, images, video, and written text. Copyright infringement is governed by strict liability; a person is guilty even if the act is committed unknowingly.

Vicarious liability is not likely to be a major concern for state government. To be vicariously liable, the state not only would need to have the right and ability to control the employee’s acts but also would need to receive a direct financial benefit from the infringement. A greater concern, perhaps, is the issue of contributory liability. This applies if a party "with knowledge of the infringing activity.... materially contributes" to it. It has been suggested that in some cases, merely knowing about an infringement and allowing it to continue is enough to establish contributory liability. This could even apply to infringing activity that may occur on the Kentucky Information Highway by non-state-government users, although the likelihood of actual liability here is probably small (Hayes).

The state's potential liability for infringement of federal copyright law is difficult to determine. It would be a valuable defense to have appropriate policies and measures in place.

Copyright law is a federal law, but the state's sovereign immunity still applies. Because the law is complex, it is difficult to determine the state's potential liability, but it would perhaps be subject to the limits imposed by provisions of the Board of Claims. It would be a valuable defense to have policies and measures in place that could counter any claim that the state knew about infringement and allowed it to continue.

Violation of Privacy or Confidentiality. State agencies maintain some information that is legally recognized as private or confidential. This includes private information about employees, those using government services, and confidential or proprietary information from individuals and organizations contracting or doing business with the state. Some of this information may be protected by federal laws, such as the Drivers Privacy Protection Act of 1994, the Family Educational Rights and Privacy Act of 1974, and the Health Insurance Portability and Accountability Act of 1996 (National Association).

State computers can be used inappropriately to access or divulge private information. Legal liability would depend on circumstances.

State computers can be used inappropriately to access or divulge private information, intentionally or not. Whether or not such action would result in legal liability, particularly as it pertains to federal law, would depend on the circumstances of the particular case. As in other cases, the best protection against the possibility is to have policies in place that control the access and distribution of this information.

Use of computers to defame, threaten, defraud, or engage in illegal operations can be the basis for lawsuits.

Defamation, Fraud, or Threatening or Illegal Activity. E-mail or network postings containing derogatory references to other persons can be the bases of defamation suits (Blaky v. Continental Airlines). This includes e-mails from supervisors regarding their employees, or e-mail from employees regarding others (Meloff v. The New York Life Insurance Company). Because an element of defamation is the publication of the defaming message, downloading or file sharing could also give rise to the claim (Morrow v. Morrow, Inc.).

It is possible that an employer would be liable if an employee were to use the employer's systems to send unsolicited mass e-mail or conduct various kinds of cyber attacks on other systems. This could be considered a form of trespass, as well as unlawful access to a computer under KRS 434 (Mooney).

Any use of computers to threaten, defraud, or engage in illegal operations, to the extent they cause damage to third persons, can be the basis for lawsuits. The more intentional or criminal in nature

that these activities are, the more likely they would be considered outside the scope of the employee's employment and the less likely the state could be held liable. Nevertheless, the state is potentially liable for these claims.

The State Might Be Liable for Improper Enforcement

Well-written policies and properly implemented procedures should reduce the state's liability from all forms of improper enforcement.

The opinion of Program Review staff is that the most likely improper enforcement risk is discriminatory enforcement. Well-written policies and properly implemented procedures should reduce the state's liability from all forms of improper enforcement. Even so, it is important that changes in the law and court decisions be monitored because efforts are being made to increase employee privacy rights (Brick; Zimmerman).

Inconsistency and Discrimination. Employers have a responsibility to enforce workplace rules and policies in a way that is reasonably uniform and not discriminatory. Employers do have some flexibility in enforcement, as long as it is not so lax or variable as to suggest there effectively is no rule or policy, and as long as it does not discriminate against any protected class. Although some employees have attempted to claim discrimination due to addiction (such as sexual addiction or Internet addiction), this has not generally been upheld (Peck and McKee 133-135). Inconsistent enforcement also might limit employer challenges to unemployment insurance claims (Mooney).

Courts have generally found that public employees do not have a reasonable expectation of privacy in their computer use, especially when they were put on notice by written policies.

Employees' Privacy Rights. Government employees enjoy greater privacy rights than do private sector employees. The 1st, 4th, 5th, and 14th amendments of the U.S. Constitution apply to government employers. It is possible that an employee disciplined for improper use could claim his or her privacy rights were violated. However, courts have generally found that public employees do not have a reasonable expectation of privacy in their computer use, even seemingly private e-mail messages, especially when they were put on notice by written policies and procedures that such activity was subject to monitoring or interception (Allred; Brick; Muhl). In cases in which a reasonable expectation of privacy was found, courts have generally held that the searches, given the governmental interests involved, were reasonable and legal under the circumstances (Allred; Leventhal v. Knapek; O'Connor v. Ortega).

Due Diligence. Generally, an employer is responsible only for employee actions of which the employer is made aware. Although speculative, there is a possibility that by introducing software

capable of analyzing all employee Internet and e-mail activity, the employer incurs a responsibility to detect and deal with inappropriate use proactively. Under this theory, the employer could be liable if it does not detect inappropriate use before damage occurs (Zimmerman).

The State Might Be Liable for Actions of Nonemployees

State government may also be responsible for the actions of nonemployees such as correctional inmates or other wards of the state.

State government may also be responsible for the actions of correctional inmates or other wards of the state. In addition, there are some settings, such as the Department of Criminal Justice Training, in which students (recruits) use state computers. Although it is not clear how much liability the state might incur for such nonemployees, the Department of Corrections' deputy general counsel suggested that inmate actions could result in some liability.

Program Review staff interviewed officials with the Department of Corrections, Kentucky Correctional Industries, Frankfort Career Development Center, and Department of Juvenile Justice. According to these officials, most inmates have no access to the Internet. One correctional facility provides highly restricted access to a legal research site. Juvenile Justice has Internet access in classrooms, restricted to a list of preapproved sites. Staff assessment is that risk of inappropriate use by inmates or juvenile offenders is very low.

As an Internet service provider, the Commonwealth might incur liability for the actions of customers, such as local governments, libraries, and schools, that receive services via the Kentucky Information Highway (Hayes; Mooney; Shipley). Further legal research into this issue is needed, but the Commonwealth can take steps to protect against this sort of liability. Proper procedures to control access by wards of the state should reduce liability. Contractual policies with customers, coupled with enforcement procedures, should reduce this type of liability.

Retention Practices for Records Can Create Liability

Open records laws usually include electronic records, so computer system contents can be considered records. Similarly, courts can subpoena electronic records as evidence.

Specific record retention periods, written into policy, can be important to satisfy legal discovery procedures and open records laws.

Specific retention periods for records, written into policy, can be important to satisfy legal discovery procedures and open records laws. This is true even for access logs that are routinely deleted as they are created. If retention periods are not written or are not specific (for example, “until no longer needed”), then normal disposal of records could be seen as an attempt to avoid discovery (United States. National Center for Education Statistics).

It is important that employees be aware of and follow retention policies for records in order to reduce the risk of liability involving open records requests and discovery of evidence.

Chapter 2

Best Practices for Managing Employees' Computer Use

Effective management of the opportunities and risks identified in Chapter 1 requires a clear, comprehensive, and enforceable acceptable use policy. It also requires procedures that thoroughly implement and enforce the policy. This chapter will develop a model of policy and procedures based on a comparison of existing policies in other states and institutions and the findings of other studies. In Chapter 3, the management of computer use in Kentucky's executive branch will be assessed based on this model.

Policy Is the Foundation of Managing Computer Use

An acceptable use policy must be clear, comprehensive, and enforceable.

A clear acceptable use policy will be easily understood, well known to the employees, and readily accessible. A comprehensive policy will cover the ways that acceptable and inappropriate use may occur, as well as the risks that need to be addressed, for the different users who may access computer resources. An enforceable policy will describe disciplinary measures and will carry contractual or statutory authority.

To develop a model to evaluate Kentucky's acceptable use policy, Program Review staff reviewed the policies of states, federal agencies, educational institutions, and private companies.

The U.S. Government Accountability Office (GAO—formerly General Accounting Office) reviewed the acceptable use policies of several corporations. The next sections of this report summarize the basic elements of acceptable use policies identified by GAO. Program Review staff reviewed 24 acceptable use policies of states, federal agencies, educational institutions, and private companies (listed in Appendix B). For each policy element, the percentage of the 24 policies containing it is listed in parentheses.

Basic Understandings Must Be Established

Monitoring employee computer use may help to limit state liability in some respects, but it is subject to its own legal limitations. Because government employers are subject to the 1st, 4th, 5th, and 14th amendments of the U.S. Constitution, state employees have privacy rights unavailable to private-sector employees. Federal laws related to wiretapping need to be taken into account. Most challenges come out in the government's favor, but this issue continues to be litigated. Agencies should be careful to ensure that their actions and policies conform to all legal requirements.

Most of the reviewed policies specify that computer resources are subject to the employer's control, that employees have no expectation of privacy, and that disciplinary action will be taken for violation of the policy. Almost all the policies also cover allowable and prohibited use.

Proprietary Assets. A policy should specify that the computing resources, data, and transactions are property of the employer and subject to the employer's control (contained in 67 percent of the 24 reviewed policies).

No Expectation of Privacy. A policy should specify that employees have no expectation of privacy in their use of computer resources, including any files stored, Internet sites visited, or messages sent or received (71 percent).

Allowable Use. A **p**olicy should specify what employees are allowed or encouraged to do with computer resources (96 percent). This statement should define incidental use, if such use is allowed.

Disciplinary Action and Investigation. A policy should specify that disciplinary measures can be taken for violation (87 percent). A brief description of the types of disciplinary action and the authority for it is used in many policies. Some policies (29 percent) also describe how investigations will be conducted and state that the results will be confidential. This is also a recommended feature (Urbaczewski and Jessup 29). In Kentucky, it may not be possible to keep the results private because of KRS 18A.020, KRS 61.870, and related statutes. Further legal research is needed on this question.

Prohibited Use. A policy should state that some uses are inappropriate and prohibited, and should describe some specific forms of inappropriate use. After reviewing policies from several states and other entities, Program Review staff compiled a list of the most common forms of inappropriate use, along with the percentage of policies that included them:

- viewing, storing, or transmitting offensive, discriminatory, or defamatory material (71 percent);
- any violation of law (87 percent);
- violation of intellectual property rights and laws, such as copyrights and patents (71 percent);
- actions that degrade overall computer system performance or expose the systems to attack (83 percent);
- any use for personal gain (79 percent);
- misrepresentation of oneself or impersonation of others (62 percent);
- promoting or raising funds for political or religious causes (47 percent of *government* policies reviewed);[4]

[4] Model policies generally did not include prohibitions on promoting political or religious causes, and they were not mentioned in nongovernmental policies.

- hacking or disrupting other computer systems (71 percent);
- aiding or allowing unauthorized persons to access computer systems (58 percent);
- starting or forwarding chain e-mails (50 percent); and
- downloading messages from personal e-mail services (8 percent).

Although only a few policies specifically mentioned downloading e-mail from a personal e-mail account, this has been identified as one of the greatest risks to system security (Kelly; United States. Department of the Treasury 2).

Details vary, but most of the policies covered how to safeguard confidential and protected information.

Protecting Sensitive Information. Policies and procedures should safeguard confidential or proprietary information. Mechanisms for doing so include

- specifying protection of proprietary information, such as industrial patents and processes (71 percent);
- specifying protection for confidential information, such as Medicaid billing or tax returns (71 percent);
- requiring procedures, such as encryption, secure storage, and secure transmission, for handling confidential/protected information (42 percent); and
- requiring procedures to protect private information contained in logs, such as Internet access and e-mail transaction logs (21 percent).

Most reviewed policies required that employees formally acknowledge that they understand and agree with the policy.

Acknowledgment by Employees. Policies and procedures should require employees to acknowledge that they are aware of and agree to the acceptable use policy (Brick; Mooney). This provides formal evidence that employees are waiving any privacy rights they might have. Program Review staff divided this category into three ways that employees are required to give this acceptance:

- a signed acknowledgment when hired or when the acceptable use policy is implemented (54 percent),
- a login notice acknowledging the policy (25 percent), and
- an annual review and acknowledgment of the policy (12 percent).[5]

Other Features of Policies Related to Computer Use. Program Review staff identified other features that were not mentioned in the GAO report or do not fit into its categories. Some, especially

[5] The GAO study indicated about 36 percent used this approach. The Program Review number probably understates its true use because it was not written into policy in many cases, and staff typically reviewed only written policies.

regarding record retention, may appear in policies other than the acceptable use policy. An organizational policy should

- specify that e-mail from employees should include a disclaimer stating that the views expressed are not those of the employer (unless otherwise authorized) and/or that the confidentiality of information in the message should be respected (included in 12 percent of the 24 reviewed policies);
- require employees to follow all computer safety and security practices (42 percent);
- require reimbursement of costs, including damages, due to incidental or inappropriate use (25 percent);
- require employee training on acceptable use (37 percent);
- give a specific retention period for e-mail messages (25 percent); and
- give a specific retention period for Internet/e-mail/workstation logs (12 percent).

Disclaimers in e-mail may have some value in protecting the employer from liability, although the value is limited (United States. General Services Administration 8). This may be particularly true when employees participate in public forums on the Internet (SANS Institute). It is important that employees do not depend solely on a disclaimer of confidentiality to protect sensitive information. All sensitive information in e-mail should be encrypted.

Although several state policies mention that costs of inappropriate use should be recovered from employees, none of the states contacted by Program Review staff has solved the technical barriers to doing so. The Kansas policy contains strong language regarding the collection of costs from employees, but a Kansas official interviewed by staff said that no agencies have implemented a billing process. Georgia and British Columbia considered billing employees and decided it was impractical. Even so, it is advisable to have an acceptable use policy that mentions the right to recover costs from employees, especially in case there are significant damages to be recovered in court.

Specific record retention periods, written into policy, are important to satisfy legal discovery procedures and open records laws. It is important that employees be aware of and follow record retention policies in order to reduce the risk of liability involving open records requests and discovery of evidence.

The Authority and Scope of Policy Must Be Established

In more than 40 percent of the states reviewed by staff, policies are based on statute or administrative regulations.

Authority To Enforce. Simply publishing an acceptable use policy may be insufficient to ensure its enforceability. Several states' policies are based on statute or are administrative regulations (accounting for 42 percent of the state policies reviewed by staff). In some cases, the users or agencies enter into a contract with the agency that provides the computer services, and the contract includes the policy.

Who Is Covered. It is clear that regular civil service employees of the executive branch are covered by state policies, but there is uncertainty about who else might be covered. Because the employer can be held responsible for anyone who is acting under the employer's direction, it is important that the policy include anyone who might be a legitimate system user.

All reviewed policies covered classified executive branch employees. Policies differed regarding coverage for other types of personnel.

Within the executive branch itself, Program Review staff identified the following types of potential users, along with the percentage of the 24 reviewed policies that appeared to apply to each:

- regular employees (100 percent);
- exempt (at-will, unclassified) employees (43 percent);
- appointed board members (17 percent);
- elected officials or executives (22 percent);
- contract staff (58 percent);
- interns (42 percent);
- volunteers (52 percent); and
- other nonemployee users, such as correctional inmates or wards of the state (13 percent).[6]

Many states operate systems like the Kentucky Information Highway, which provides services to other customers. As mentioned in Chapter 1, such customers may raise a liability risk for the state. To reduce this risk, most states' provider contracts include a statement binding these customers to the same acceptable use policy as that used by the government.

Taxpayers are exposed to risk through computer use in all branches of government. Most states have not addressed this issue centrally but depend on each branch to establish its own practices. Other

[6] In interpreting the 24 reviewed acceptable use policies, staff did not include a group unless it was specifically mentioned or clearly covered. In practice, some of the groups may be covered by more policies than the percentage indicated here.

states have taken action to make policies and procedures uniform across all branches.

Tennessee Code §4-3-55 created a Tennessee Information Systems Council with authority to establish policy for all branches of state government. The council includes members of the legislative, judicial, and executive branches, as well as representatives of state employees, private industry, and the state regulatory authority.

Kansas Statute 75-7201 and related statutes established an Information Technology Executive Council with authority to issue regulations that cover all branches of government. The council includes members of the legislative, judicial, and executive branches, as well as representatives of the state university system, educational system, local governments, and private industry.

Staff review of the constitutional issues in Kentucky concluded that it was unlikely that such a body could be established with statutory authority over all branches of government. However, because of the Kentucky Information Highway, there is another avenue for government-wide enforcement of the acceptable use policy.

In North Carolina, Delaware, and some other states, the statewide government network supplies services on contract with each state agency, and the contract stipulates that their acceptable use policies must be followed. In this way, a central policy can be enforced on all branches of government without creating an overarching governing body. On the other hand, the consequences that the service provider can impose are limited to cutting off a user's (or agency's) service. Each agency or branch of government is independently responsible for applying its own consequences.

Incidental Use Practices Vary

Three quarters of the reviewed policies allowed personal computer use that did not result in a cost to the employer.

Of the policies reviewed by staff, 78 percent specifically permit incidental personal use, while 17 percent specifically prohibit it. In all cases, incidental use is defined as use that does not result in a net cost to the employer. Whether incidental use is desirable depends partly on whether allowing it costs less than preventing it. The decision about incidental use also needs to consider incidental use of the office telephone, fax machine, and other office equipment.

Allowing incidental use does increase some of the risks described in Chapter 1, unless it can be managed reliably. Allowing incidental use might increase employee satisfaction—and productivity in some cases (Websense, "Desktop"). If an employee can run errands online, such as checking on child care, scheduling dinner, checking on stocks, then the employee may worry less about personal issues, focus more on work, and even take less time during lunch to do some of those same errands.

A Texas policy review team stated that "E-mail & Internet personal use policies should be neither more nor less restrictive than policies for personal use of other communication mediums such as telephones, digital pagers, etc." (State of Texas). This is a theme repeated in several sources reviewed by staff.

Further, the Texas team determined in 2002 that "prohibiting personal use of e-mail & Internet is difficult, if not impossible, to enforce" (State of Texas). The newest technology that controls Internet and e-mail access is much improved but still imperfect. Content security management systems can do a good job of limiting Internet access to approved types of Web sites. Still, they cannot tell whether an employee is visiting an approved site for work or personal purposes. They are even less capable of detecting and preventing personal e-mail use.

The Kentucky Department of Criminal Justice Training installed the Websense® CSM package to control employee access to the Internet, a practice that shows some promise. The Websense system categorizes Web sites and allows administrators to establish rules stating whether a category is acceptable for work-related use, for incidental use only, or not permitted at all. When a user wants to visit a site for incidental use, the user asks the system for a five-minute block of time during which access to nonwork sites will be allowed. A user is granted a weekly quota of incidental use time by management, from which the five-minute blocks are taken.

The positive aspects of this practice include employee accountability and self-management, as well as a distinction between work-related and purely incidental categories of Web sites. However, as with other such systems, the Websense content security manager cannot tell whether an employee is visiting a work-approved site for work or personal purposes.

It is also possible to have different approaches for use of the Internet and e-mail. For example, incidental Web use could be prohibited, but incidental e-mail use could be permitted. Because it

is somewhat easier to manage Internet use and the Internet is not a person-to-person communications medium, this approach can be presented as a fair policy.

E-mail use is even more difficult to control via an information technology tool. Although content security management systems can check e-mail for key words that indicate personal use, this method is likely to miss many personal messages and to mistakenly flag business messages as personal. Also, e-mail use is directly analogous to telephone use and policy should treat it accordingly.

No matter what tool is used, and whether or not incidental use is allowed, best practice has to involve management. IT tools can provide feedback to managers and to individual users about surfing and e-mail patterns so that supervisors can spot questionable activity and employees can police themselves.

Most experts who are connected with content security management and similar products seem to focus on the risks of incidental use and on the possibility of prohibiting it. Most human resource consultants seem to focus on the benefits and management of incidental use and on the difficulty of eliminating it fairly.

The staff recommendation for best practice is that incidental use of the Internet and e-mail be allowed and carefully managed. This position is based on the fact that

- no technological tools are available that can eliminate incidental use; and
- the computer acceptable use policy should be consistent with policies on acceptable use of telephones, copiers, and other office equipment.

Top Management's Commitment Is Required

All levels of management should understand and commit the resources required to implement the acceptable use policy successfully.

A good policy will fail unless it has the support and commitment of all levels of management. Whoever spearheads the implementation of the acceptable use policy must work to gain the understanding and commitment of top management, information technology management, human resource management, and the management of all departments or agencies. Managers and staff must be convinced of the importance of the policy and the need to carry out acceptable use procedures on a day-to-day basis. Acceptable use policies and procedures must have priority and funding.

Acceptable use policies and procedures do carry a cost in terms of information technology expenses (software, hardware, and staff time), human resource staff time, and supervisory effort. In addition, employees should receive initial and continuing education on sound computer use practices, which will consume some employee time.

Human Resource Approaches Are Essential

There is a consensus that effective implementation of a policy must include good human resource procedures. A successful strategy consists of specific procedures to help prevent improper computer use and to develop a workplace culture conducive to acceptable use.

Virtually all the groups involved—from security software vendors and information technology staffs to human resource consultants and personnel staffs—agree that successful implementation of a good policy depends on good HR procedures. Many experts recommend that the human resource office create and maintain the acceptable use policies and procedures, with the advice of IT and legal staff.

Best human resource practice for managing acceptable computer use overlaps with best practice for personnel management in general. The three main goals of HR management are to provide the best possible services, maximize employees' commitment, and maximize productivity (Kopelman). Computer use may advance or hinder any of these goals.

Maximizing Employees' Commitment

The goal of maximizing employee commitment generally does not involve computer use in itself. Rather, the approaches to managing computer use can greatly affect employee commitment, and employee commitment can strongly influence the success of computer use management. Many of the relevant HR practices focus on this goal.

Prevention. Steps such as pre-employment screening, background checks, and skilled interviewing help ensure that good employees are hired and that employees are fully aware of their responsibilities. Such employees should be more likely to use computers appropriately in the first place. Procedures relevant to computer use should also provide for

- thorough orientation for new employees, including training specific to the computer acceptable use policy;
- written acknowledgment of the policy by new employees;
- mentoring new employees to ensure the policy is understood;

- identifying staff to whom an employee may report problems, obtain resources, and get information and assistance with computer use issues;
- training employees in best practices for handling data, browsing the Web, using e-mail, and recognizing and dealing with security threats;
- reminding employees of the policy in publications, on Web sites, and via e-mail; and
- requiring annual review and acknowledgment of the policy by the employee.[7]

Workplace Culture. Because inappropriate computer use may be seen as theft of time and services, increased employee commitment to the workplace is likely to reduce inappropriate use. The methods of managing employee theft also apply to managing the acceptable use policy. Many experts agree that problematic employee behavior can be minimized, and desirable behavior maximized, by developing a positive workplace culture.

In the absence of a positive culture, disgruntled employees—whether because of dissatisfaction with the policy or workplace conditions in general—can create costs in all of the risk areas. This supports the need to emphasize a culture of respect and trust.

There is evidence that using a zero-tolerance approach and excessive controls can work against a positive workplace culture and lead to dissatisfaction and turnover (Moorman and Wells). Nonetheless, there are positive ways to present controls so that employees will see them as justified and fair. The authors found that employees perceived electronic controls as fair when they received clear, understandable, and useful feedback about their own performance; and have a responsive system for challenging or giving feedback about the controls.

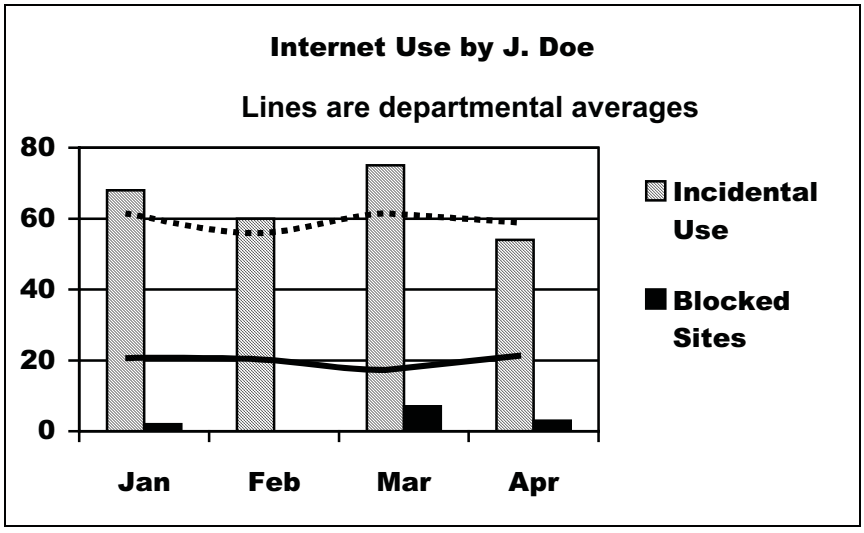
In addition, Moorman and Wells noted that when employees saw electronic controls as fair, they also were more likely to act in positive ways, such as being helpful, considerate, cooperative, persistent, motivated, and disciplined.

Charts and tables that show progress toward objectives can provide valuable information to employees and provide useful context. An example of feedback for a hypothetical individual employee is given in Figure 2.A. It shows incidental use and attempts to visit blocked sites compared with the averages for the employee's

[7] Staff compiled the procedures from several sources, including Allen et al. 6-7; Cooper et al. 154; Mullich; Niehoff and Paul 61; and Peck and McKee 136-137.

department. The employee can see that his or her incidental use was above average until the last month. The employee's attempted visits to blocked sites have generally been better than average. Such feedback demonstrates to the employee that monitoring is going on and gives the employee a way to judge his or her performance but without reporting private or embarrassing information. Similar information could be provided to departmental employees as a group. Employees working as a team might think about how to deal with any problems. Research suggests that posting information like this can motivate employees to work toward improving departmental results (Oliphant and Oliphant).

Figure 2.A
Illustration of Individual Employee Feedback



Source: Illustrative data devised by Program Review staff.

Maximizing Productivity

The goal of maximizing productivity also benefits greatly from computers, but inappropriate computer use may have its greatest effect in this area.

An HR representative interviewed by Program Review staff described the company's procedure when an employee is suspected of excessive, but not illegal, personal use. If the employee has met his or her work goals, the manager is advised to increase the employee's workload. If the employee has not met work goals, the employee is advised to spend more of his or her time on work.

The best method of dealing with productivity problems is a performance review system with clear and measurable goals individually developed with the input of each employee. To the extent that IT tools are used to monitor and control productivity, HR must ensure that the tools provide understandable and useful reporting to employees and that managers solicit and listen to employee feedback.

As a practical matter, employees need a rapid way to gain access to blocked sites if there is a legitimate business reason. In the absence of such a procedure, there may be delays or lost productivity and employees might try to circumvent the block by themselves.

Managing Computer Security Through Human Resource Approaches

Employee education is critical so that proper procedures can be utilized to maintain the security of computing resources. Employees should understand that they must share responsibility for computer security.

Many employees are not well informed about or motivated to follow best practices (Bennett). However, employees are crucial to maintaining the security and integrity of computing resources: "Without active employee involvement and follow-through, a data security policy is little more than a piece of paper or a page on an intranet site" (Lyon and Wugmeister).

The Internet Security Alliance made training one of its top 10 recommended information security practices (Allen et al. 6).

Training should include ways to maintain security and minimize spam. Some relevant topics are

- using the Internet and e-mail,
- storing and transmitting confidential data,
- keeping workstations and passwords secure, and
- recognizing and dealing with security breaches.

A crucial element of security training is to recognize and defeat social engineering attacks. In recent years, social engineering has been used in some cases to entice users into opening e-mail attachments that activated computer worms. Having an employee culture that creates awareness of security risks and having appropriate training in recognizing and avoiding them is essential (D'Agostino).

The Internet Security Alliance stated that users should have ready access to reliable computer systems support personnel (Allen et al. 7). In addition, experts advise having a single well-known channel or hotline to which employees can turn when they have any kind of computer use or security question or when they need to report any

kind of computer-related problem (D'Agostino). The channel should be responsive and timely, or employees will be tempted to circumvent safeguards.

Environmental Strategies

There are some strategies for managing computer use through the structure of the work environment. Two such strategies are the open office and eliminating Web access.

In its new facility, the Transportation Cabinet created an open office for most employees. Workstation monitors are visible to everyone in the area, which reduces the opportunity for hidden misuse. A more extensive policy could require all monitors to be visible from the door of individual offices or cubicles. An issue that must be dealt with, however, is that confidential data might be displayed on the monitor.

Another strategy recommended by the Transportation Cabinet's Inspector General's office, and suggested by experts, is to eliminate Internet access for employees who do not need it (Peck and McKee 137). Not everyone with a workstation, or even everyone with e-mail, needs to use the Web. Having a common workstation in a public area can provide Internet access for those who do not have it on their workstations.

Information Technology Tools Have Strengths and Weaknesses

The main uses of information technology tools are to regulate use of the Internet, e-mail, local networks, and workstations.

Implementation of an acceptable use policy requires information technology tools. Some employees will disregard the policy if they can, especially when seeking sexual materials (Peck and McKee 130). IT methods can place virtual roadblocks in their path. The main uses of information technology are to regulate use of the Internet, e-mail, local networks, and workstations.

IT hardware and software tend to operate continuously, uniformly, and reliably, thus avoiding many human failings. Computer systems can fail to work properly, however. For example, the U.S. Treasury Department found that Internet-blocking tools used by the Internal Revenue Service failed to work when they were overloaded, which happened on several occasions (United States. Department of the Treasury 5).

Information technology also cannot make intelligent judgments. For instance, Internet blocking may be set up to allow an employee to access eBay. At any given time, the employee may be conducting legitimate business procuring equipment or selling surplus; or the employee may be running a side business. The blocking software cannot tell the difference.

Information technology methods require human assistance to create their rules, verify their operation, and monitor for situations that the system cannot handle.

In all cases, IT methods require human assistance to create their rules, verify their operation, and monitor for situations that the system cannot handle. All employees, not just IT and HR staff, should be alert for signs that the tools are not working properly.

Managing Internet Use

Access. To manage user access to the Web, acceptable and unacceptable Web sites must be identified. If access is to be filtered, then there must be a way to block access to sites identified as inappropriate. In the past, this generally required IT staff to create and maintain a list of prohibited sites, which quickly exceeded available staff time. Knowing this, Web site owners would change their Internet addresses regularly, allowing users to get around the filters.

Recently, effective content security management systems to manage employee access to the Web have become available. These systems include a number of functions that go beyond control of Internet access. Content security management is covered throughout this chapter.

Internet access can be managed through a content security management (CSM) system. The system's vendor maintains an up-to-date database of Internet addresses that the information technology administrator can use to block access.

Perhaps the most important feature of content security management is that the vendor maintains a centralized database of Internet addresses, all classified as to their content. At frequent intervals (once or more per week), the vendor updates the database of addresses. The information technology administrator can block or allow access to any of these categories or to specific sites within a category for all users, some users, or individual users. If a user tries to access an unclassified site, the content security system automatically sends the Web address to the vendor who classifies it in the next update.

Content security management can prevent most inappropriate use by blocking categories prohibited by the acceptable use policy. For users who have a legitimate business reason to access one of those sites, the IT administrator can grant exceptions. That user could then visit the site for personal reasons, but the system can produce reports that allow managers to know what the user is doing.

Typically, a CSM system has security features such as antivirus protection, and can also help manage bandwidth capacity.

Security. In addition to managing employee access to the Web, Internet management must protect the systems themselves. Employee browsing, mistakenly or not, can invite an attack on the system. As the first line of defense against hackers, adware, and spyware, tools such as firewalls and antivirus software are crucial. Content security management typically will include integrated antivirus and firewall features. In addition to thwarting attacks, the system should provide information on how the attack was started and what, if anything, the employee did to trigger it. Management can use this information to educate or discipline the employee.

Capacity. Managing bandwidth is important because exceeding bandwidth capacity can bring Internet access to a halt. Content security management can automate bandwidth management, ensuring that capacity is never exceeded. Some Web requests can be denied temporarily, based on a priority list, while the system as a whole continues to function.

Managing E-mail, Spam, and Messaging

E-mail. E-mail has created a new medium for business and personal communication but has also created new risks. E-mail can encourage unproductive use of time; use up bandwidth; fill up servers; and carry destructive, illegal, or confidential attachments.

CSM systems can block or monitor e-mail content and addresses, filter spam, and control instant messaging and peer-to-peer file sharing.

Information technology methods have existed for some time to manage e-mail capacity, usually by limiting the size and kind of attachments and number of messages that a user can store or send. CSM systems add the ability to block or monitor content and e-mail addresses. They do so by scanning messages for key words and phrases and by checking their origin and destination against lists of allowed or prohibited addresses.

Firewalls and antivirus software have been indispensable for protecting systems from cyber attacks via e-mail. CSM systems typically include this capability as well. Such a system should be able to block most attacks and produce reports that managers can use to correct any problematic behavior by employees.

Spam. The volume of spam in general is increasing, although the number of unsolicited e-mail ads sent to business addresses may be less than that sent to personal addresses (American Management Association 5). Software can help identify spam but the employee usually at least has to look at these messages to verify that they are spam. The primary productivity gain is that the spam is

concentrated in one place. CSM systems typically include spam filtering.

Peer-to-Peer and Instant Messaging. With the growth of the Internet, new messaging methods have evolved. Instant messaging, similar chat systems, and peer-to-peer file sharing not only have great potential to waste time and resources, but they can carry cyber attacks. CSM systems typically allow administrators to eliminate or control these types of messaging.

Management of Workstations and Local Networks

The basic goals of workstation and local network management are to prevent the storage of prohibited files and the installation of unauthorized software or hardware. Secondary goals include accounting for system usage and protecting systems from cyber attack.

Information technology tools are available to manage files on computer workstations on a network.

File Management. Information technology is available to scan workstations and servers on the local network for files that fit certain patterns. Very large files, prohibited types of files such as video and unauthorized software can be discovered.

Capacity Management. In the same way that Internet access can halt when bandwidth capacity is exceeded, local file servers can crash when their storage capacity is exceeded. IT staff have often placed limits on the amount of storage an individual can use, but this has not kept file servers from filling up.

Storage resource management software has become more effective. Such systems can prevent users from storing files that violate policies and can interact with users to let them know when they are approaching their space quota. Storage resource management software can ensure that file servers never fill up and crash.

Security Management. At this level, the most likely form of attack is from the careless or uninformed user or a malicious employee. In either case, an attack can come from an infected diskette in a workstation or a portable computer plugged into the network. It is also possible for an infectious e-mail to slip past statewide defenses onto a workstation. Antivirus software at the local network and individual workstation levels is the final line of defense against cyber attack.

IT administrators also have means to protect certain information that is stored on the local systems. Passwords and security rules to

control access keep some attackers from deleting or copying sensitive files. File encryption can be used to obscure the contents of sensitive files.

In order to ensure that employees do not accidentally or deliberately disable security features, administrators typically remove users' rights to install new software or hardware on local workstations. Further, they can, and usually do, remove users' rights to modify sensitive workstation features, such as the password-protected screen saver, antivirus software settings, and the system clock.

Policy and Procedures Must Be Measured and Evaluated on a Routine Basis

The effectiveness of the acceptable use policy and associated procedures should be measured and evaluated. Policy and procedures should be reviewed regularly for legal compliance and best use of technology.

It is good management practice to measure and review the results of any important business process. Thus, the effectiveness of the acceptable use policy and associated procedures should be measured and evaluated. Policy and procedures should be reviewed regularly for legal compliance and best use of technology.

Suggested outcome measures are listed below. These lists are not intended to be complete but rather to indicate a direction for evaluators to pursue.

The effectiveness of human resource procedures should be assessed by anonymous surveys of employees that ask about issues related to the acceptable use policy, such as

- knowledge and level of acceptance of the policy,
- practical knowledge of good policy and security practices,
- suggestions for improving the policy and related procedures,
- suggestions for improving productivity and service quality, and
- awareness of violations of the policy.

Human resource staff should track compliance with the acceptable use policy by keeping statistics on allegations and confirmations of violations, disciplinary actions taken in confirmed cases, and time from allegation to disposition of cases.

Information technology procedures also require benchmarking and trend analysis of several measures, including

- local network file storage used;
- number, type, and size of files stored on file servers;
- bandwidth used;

- number and size of e-mails sent and received;
- number and size of e-mail attachments sent and received;
- number of infected e-mails received;
- number of e-mails identified as inappropriate by category;
- amount of spam received;
- number of sites visited by category; and
- number of attempts to visit blocked and unclassified sites.

Information technology systems should also be tested.

- Routine vulnerability testing of security systems should assess the alertness and responsiveness of employees to cyber attacks and social engineering espionage.
- Acceptable use policy procedures should be tested from the inside by staff who attempt to "break out" of the built-in restraints.
- Information technology tools should undergo stress tests to ensure they do not fail under heavy loads.

Both the law and technology of computers change rapidly. Policy and procedures should be reviewed at least annually for compliance with new legislation or case law and for best use of new technology. Although only 12 percent of the policies reviewed specifically included a review period, this practice is recommended by several experts (Cooper et al. 154; Mooney 3, 16).

Chapter 3

Kentucky's Management of Acceptable Computer Use Is Improving

Agencies' Past Efforts Have Been Inconsistent

An acceptable use policy for all executive branch agencies has been in place since 1996.

An acceptable use policy for the Internet and e-mail has been in place since 1996 (Commonwealth of Kentucky. Commonwealth Office of Technology). GOT-060 (now CIO-060) established policy for the executive branch, but agencies were permitted to add more restrictions. Standards for other aspects of computer use have been in place since 1999.

Some agencies have invested in proxy servers or content security management in order to control employee access to the Web. COT provided a list of six major agencies with proxy servers as of November 2003, two of which were not used to filter access. Program Review staff identified additional proxy servers used for filtering in four departments now in the Justice and Public Safety Cabinet. At least some of the remaining agencies did not manage Web access in this basic way.

Some agencies described routine—sometimes daily—management review of computer usage reports. As of August 2004, 6 of 11 major agencies indicated using these reports at least monthly, although it was not clear how many were doing so in 2003. An official of the Personnel Cabinet told staff that some agencies did not agree that computer use management was worth the cost and some agencies had difficulty finding the funds. Staff found that some agencies did express concern about the costs associated with obtaining hardware and software and paying for the labor to set up and maintain filtering systems.

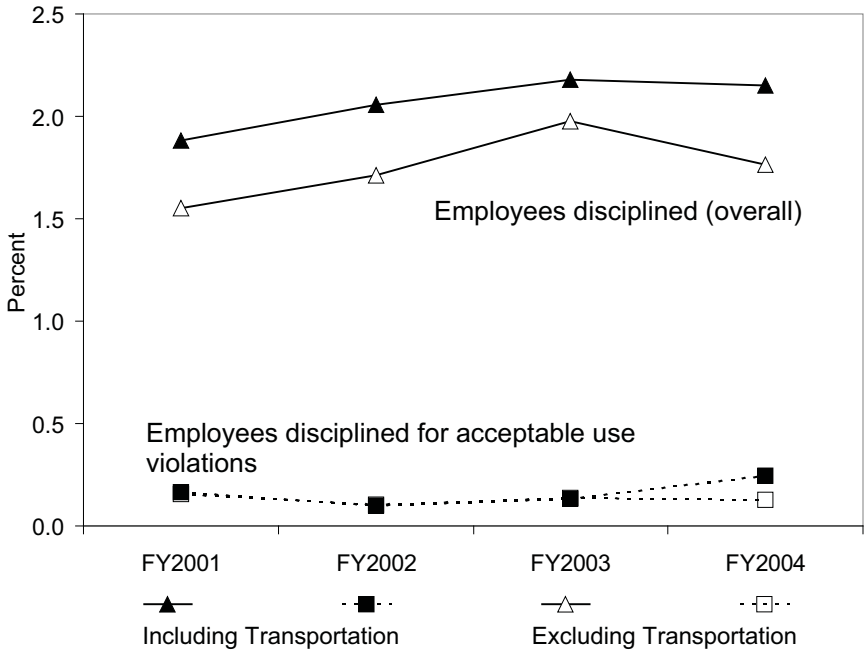
Maintaining a conventional proxy server blocking list is labor intensive. However, the agencies that installed CSM packages reported high levels of satisfaction and very little staff time required to support the system.

Personnel Actions Related to Inappropriate Use Have Been Infrequent and Stable Over Time

Information about past computer use problems is limited. Staff estimated that well less than one-half of 1 percent of employees per year have been disciplined for improper computer use.

Historical information about the extent of computer use problems in Kentucky government is lacking. Internet access logs are not kept, and usage statistics are not available. There is no information on productivity gains or losses associated with computer use. Having no direct evidence of usage patterns, staff attempted to gauge the trend by asking each agency to provide the number of employees disciplined in the past four fiscal years. The results are shown in Figure 3.A.

Figure 3.A
Percent of Executive Branch Employees Disciplined
FY 2001 to FY 2004



Source: Agency numbers compiled by Program Review staff.

Because agencies do not keep this sort of information readily accessible, and because the recent reorganization has combined different HR offices, some of the numbers obtained were estimates. These numbers represent only those employees who were caught, leaving the number unknown of employees who may have misused computers during this time. The recent investigation at the Transportation Cabinet, which led to a large number of personnel actions, probably greatly exceeded the number that

would have been brought otherwise. Therefore, Figure 3.A shows actions with and without the Transportation Cabinet's numbers.

These numbers, although of limited value, indicate that violations of the acceptable use policy probably have remained steady for the past four fiscal years. The percentages are truly tiny, representing fewer than 1 in 800 employees, but these numbers reflect only the known violations. Unfortunately, there is no way to determine how prevalent inappropriate use actually is in Kentucky state government.

A Centralized Approach Is Being Implemented

In recent years, the Commonwealth Office of Technology has adopted a number of strategies to improve computer systems management across the executive branch. To promote communication and coordination, COT has issued policy, set standards, held monthly meetings of agency chief information officers, developed a Web site, and published a series of newsletters. Beyond that, COT for some time has been moving toward a centralized information technology approach to manage computer use.

Based on a pilot study, a five-year $1.9 million contract was awarded in 2004 to implement the Webwasher® content security management system.

In 2002, COT formed a Content Security Management Team to study the benefits of combining antihacking, antivirus, antispam, e-mail filtering, and Internet filtering into a single management tool at the state level. This would eliminate the need for each agency to purchase and maintain its own filtering system.

After reviewing the available products, the team conducted a 60-day pilot of the Webwasher® CSM in the winter of 2002-2003. The pilot was considered a success and was followed by a Request for Proposal in November 2003. In April 2004, COT announced it had signed a contract with Network Appliance, Inc. for a CSM package including the Webwasher software. The total cost of the contract is $1.9 million ($380,000 per year for five years). COT implemented the system in some agencies in May, with the new system expected to cover all agencies by the end of September 2004.

The new strategy has had significant involvement from other agencies, most notably the Governor's Office. The Personnel Cabinet and the Finance and Administration Cabinet have also taken major roles.

The task force on acceptable use includes staff from the Governor's Office, the Finance and Administration and Personnel Cabinets, and COT. An objective of the task force is to write a regulation that will embody the acceptable use policy.

Human resource, legal, and IT staff from the three agencies and the Governor's Office have formed a task force on acceptable use of the Internet and e-mail. Besides guiding the implementation of the CSM, this task force has three other objectives:

- write a regulation that embodies the Internet and e-mail acceptable use policy,
- include awareness of and compliance with that policy as part of employee evaluations, and
- foster employee awareness in general.

Program Review staff found that this strategy is commendable for several reasons:

- It has commitment from the highest levels of state government.
- It utilizes state-of-the-art technology to block inappropriate access to the Internet and to monitor e-mail.
- The technology operates without action by individual agencies, yet allows agencies to add stricter controls.
- It includes procedures to inform and remind employees about the policy.
- It will carry the force of law through an administrative regulation.

Kentucky's Acceptable Use Policy and Procedures Have Many Positive Features

This review covers several policies. Standards relevant to employee computer use also were included in the review. The work of the task force on acceptable use policy did not extend to some of these areas.

At the time of this writing, the task force has not completed drafting the regulation. Because the regulation will be based on CIO-060, this report will review the existing policy in lieu of the future regulation. Staff included CIO-079 (policy requiring a login notice); CIO-082 (policy on vulnerability testing); and Enterprise Standards 3550 (storage networks), 4060 (e-mail record retention standard), and 5515 (secure transfer of data) in the review because they are relevant to acceptable use. (Appendix C contains these documents.) The following discussion also includes Personnel Cabinet strategies for implementing the policy.

In preparing this report, staff used a broad conception of what is relevant to the issue of acceptable use, much broader than the scope of CIO-060 and the planned regulation. In this chapter, some recommendations will apply to other policies and standards that were beyond the mandate of the task force on acceptable use policy. This should not be taken as a criticism of the task force's work.

Summary of Policy and Procedure Features

Table 3.1 evaluates the acceptable use policies and procedures based on the best practices model developed by Program Review staff.

Table 3.1 summarizes the best practices model developed by Program Review staff. Items with checkmarks are included in either the Internet/e-mail acceptable use policy, related policies, or procedures to implement the policy. Items with numbers in parentheses are explained further in corresponding notes following the table. Items with question marks need further clarification or research.

Table 3.1
Comparison of Kentucky Policies and Procedures With Best Practices

General Policy Contents	
✓	Statement of employer ownership of computer assets
✓	No expectation of privacy
✓	Allowable employee use encouraged or explained
Y	Incidental use permitted (Y) or prohibited (N)
(1)	Disciplinary action described
(2)	Description of investigative procedures and privacy of findings
Types of Improper Use Described in Policy	
✓	Viewing, storing, or disseminating offensive, discriminatory, or defamatory material
✓	Violating laws in general
✓	Violating intellectual property laws (copyrights, patents, trademarks)
✓	Using services/resources that could degrade performance or expose systems to attack
✓	Using resources for personal gain
✓	Misrepresenting oneself or impersonating others
✓	Promoting or raising funds for political or religious organizations (applies to government entities)
✓	Hacking or disrupting other computer systems
	Aiding or allowing an unauthorized person to have access to systems
✓	Starting or forwarding chain e-mails
	Downloading messages from personal e-mail services
Protecting Sensitive Information	
✓	No unauthorized release of proprietary information (e.g., intellectual property)
✓	No unauthorized release of confidential information
(3)	Procedures for handling confidential/protected information (e.g., encryption, secure storage, secure transmission)
	Procedures to protect private information contained in system logs (e.g., Internet access, e-mail transactions, other computer/network activity)

Acknowledgment of Policy	
✓	Signed employee acknowledgment of policy
✓	Notice of acceptable use policy at login
✓	Annual review and/or acknowledgment of policy by employee
Other Policy Elements	
(4)	Using disclaimers in all messages (e.g., views expressed do not represent those of the Commonwealth, contents are confidential and intended only for the recipient)
(5)	Following all computer safety and security practices
	Reimbursement of costs (including damages) due to incidental or inappropriate use
	Employee training on acceptable use, including justification for policy
(6)	Specific retention period for e-mail messages
	Specific retention period for system logs
Authority and Scope of Policy	
✓	Carries authority of statute or administrative regulation
✓	Covers regular employees (merit, classified)
?	Covers "exempt" employees (nonmerit, "at-will," unclassified, etc.)
?	Covers appointed board members
?	Covers elected officials or executives
✓	Covers contract workers
✓	Covers interns
✓	Covers volunteers
?	Covers correctional inmates and other wards of the state
Implementation of Policy (Human Resource)	
	Prevention strategies
	Training employees on reasons for the acceptable use policy
	Detecting personal problems and referring to assistance
	Employee involvement in development of policy
	Ensuring there is an avenue for employee feedback and reporting of violations
	Training supervisors to build loyalty, dedication, and motivation
	Uniformity of investigative and disciplinary procedures within administrative units
	Reporting the level of inappropriate use to work groups
	Reporting usage information to individual employees
(7)	Employee evaluations with clear and measurable goals related to the acceptable use policy
(5) (8)	Employee training on safe practices for Internet surfing, protecting e-mail addresses, protecting local systems, recognizing and reporting problems including social engineering attacks
	Universally known, accessible, and responsive computer assistance and problem-reporting process
	"Open office" (monitors visible to passers-by)
	Web access provided only to those who need it for work

Implementation of Policy (Information Technology)	
✓	Use of a content security management system to control Web access, e-mail content, cyber attacks, and bandwidth usage
(9)	Use of a storage resource management system or other means to control use of storage, storage capacity, and file access rights
(10)	Workstation security, including antivirus software and limited user privileges to prevent installation of unauthorized software or hardware and to prevent modification of sensitive system settings
Measurement and Evaluation	
	Solicitation of employee feedback to measure acceptance and effectiveness of policy and procedures
	Statistics on allegations of policy violations and disposition of them
(11)	Statistics from IT management tools
(12)	Vulnerability testing, including employee alertness and responsiveness to cyber attacks and social engineering espionage
	Testing IT filtering/blocking processes
	Stress testing IT management tools
	Annual reassessment of policies to ensure they reflect the latest legal and technological changes

(1) CIO-060 mentions disciplinary action as "up to and including dismissal." This was true of many other polices reviewed, but best practice indicates that a list of possible actions is desirable (e.g., reprimand, demotion, etc.).

(2) A description of the investigative process might include whether the employee will be informed when an investigation begins, examples of actions such as monitoring or seizure of data, and reference to disciplinary procedure documentation. Privacy of findings of investigations may be limited under Kentucky law. Further research is needed to determine how much assurance of privacy, if any, is allowed under KRS 61.878 and KRS 18A.020.

(3) CIO-060 mentions encryption for e-mail transmission of confidential information. Enterprise Standard 5515 requires use of secure Internet transmission for sensitive data. Staff are not aware of standards for secure file transfer, secure storage such as encryption, or access permissions

(4) CIO-060 requires a confidentiality statement but not a disclaimer that views do not represent those of the Commonwealth.

(5) GOT-067, the COT security manual, covers this issue but applies only to COT employees. Agencies are encouraged, but not required, to adopt it.

(6) Retention periods for e-mail are determined by the nature of its content and are governed by retention schedules issued by the Kentucky Department for Libraries and Archives. Individual agencies are responsible for classifying e-mail and specifying the retention period within these guidelines.

(7) Individual agency personnel offices have considerable autonomy in adopting strategies. The Personnel Cabinet has endorsed these items and encourages agencies to adopt them.

(8) CIO-060 states in general terms, but is not specific, that supervisors are to obtain needed training for their staff.

(9) Enterprise Standard 3550 encourages the use of storage management systems. Program Review staff did not ask agencies about this topic. Further assessment is needed.

(10) COT does not have control over users' workstations and does not appear to have guidelines for agencies on this matter. Program Review staff found that most agencies claim to control their workstations appropriately.

(11) COT keeps records only on bandwidth usage.

(12) CIO-082 does not include testing the ability of employees to notice and react to cyber attacks or social engineering espionage, applies only to "critical systems," and is mandated only once every two years.

Going Beyond the Best Practices Model

CIO-060 contains the following helpful additional elements that were not part of staff's best practices model.

- "Making fraudulent offers of products, items, or services originating from any Commonwealth account" is prohibited.
- "Developing or maintaining a personal Web page on or from a Commonwealth device" is prohibited. This appears to be a positive addition because some employees might consider a personal Web page as falling under incidental use.
- "Use of peer-to-peer (referred to as P2P) networks" is prohibited. This appears helpful as a clarification, although any listing of specific networks must be kept current.
- Agencies are prohibited from reselling Internet access and must obtain COT approval before using the Internet commercially. This provides a helpful guideline for agencies, although it might be more appropriate in a service provider contract.
- Agencies are prohibited from accepting paid commercial advertising on a Web site, a federal requirement when states use .gov domain names. This, too, seems more a service provider contract issue than an employee acceptable use issue, but it is helpful agency guidance.
- "Auction services such as eBay unless the activity is for Commonwealth business" are prohibited. The policy already prohibits use for personal gain, but this may have been intended to prohibit buying on auction sites. This should be clarified and accompanied by an explanation of the state's reasons if it is intended to exclude buying. Supervisors will need to be vigilant to prevent employees who have access to auction sites from using them for personal gain.

CIO-060 allows special exceptions to be granted when an employee's job requires him or her to perform an otherwise prohibited activity.

Costs and Risks Have Been Reduced by Kentucky's Acceptable Use Policy

The adoption of the Webwasher® content security management system should simplify the management of Internet and e-mail usage across agencies. Agencies' costs for hardware, software, and information technology staff should be reduced. The use of the system to eliminate offensive Web sites and e-mail should greatly reduce the risk of adverse publicity and legal liability.

The adoption of the Webwasher® CSM should greatly simplify the management of Internet and e-mail usage across agencies. If agencies accept the central solution as adequate, this should reduce their costs for hardware, software, and information technology staffing.

Further, the use of the CSM to eliminate offensive Web sites and e-mail should greatly reduce the risk of adverse publicity and legal liability. Limiting access and increasing awareness that the CSM system will track everyone's Internet use and e-mail should reduce overall personal use of computer resources, saving some capacity costs.[8] Combined with good human resource management, the CSM strategy might result in greater productivity, perhaps the largest dollar savings of all. The CSM's integrated antispam and security features help address costs in these areas as well. The Commonwealth Office of Technology's use of CSM with other security tools is an industry best practice.

Concerned that correctional inmates could present a risk, Program Review staff interviewed officials with the Department of Corrections, Kentucky Correctional Industries, Frankfort Career Development Center, and Department of Juvenile Justice. Staff concluded that the procedures in these agencies already did a good job of minimizing the risks of inappropriate computer use. The statewide CSM and management awareness can only improve the situation.

Some Aspects of Policy Could Be Improved

Kentucky's acceptable use policies are thorough and comprehensive. There is room for improvement, however.

Table 3.1 demonstrates that Kentucky's policies related to acceptable computer use are thorough and comprehensive, matching up well with model policies reviewed by staff. Some areas of policy should be considered for addition and some existing policies could be improved.

Program Review staff recognized that the original mission of the task force on acceptable use policy was Internet and e-mail policy. Best practices indicate that organizations should consider all policies, standards, and procedures that relate to employees' use of computer systems, including the ways employee use affects system

[8] COT estimated that it would recover most of the $1.9 million CSM contract expense as cost avoidance from bandwidth reduction alone over five years.

security. Staff suggest that the task force on acceptable use policy expand its mission accordingly.

E-mail is subject to open records laws and for use as evidence through the legal discovery process. Destruction of e-mail records could be seen as an attempt to avoid discovery. Specific, written retention periods can protect against this risk. Although COT standards and Kentucky Department for Libraries and Archives policies apply to retention of records, they are not specific, and all agencies are responsible for writing and enforcing specific retention policies. All agencies need to ensure that their retention policies include a minimum time period for all forms of e-mail, but especially for personal or transient e-mail. Such temporary records probably should be destroyed within one day unless needed longer.

Under "Responsibility for Compliance," CIO-060 refers to "executive cabinets" rather than agencies. This technicality could leave out the Departments of Military Affairs and Veterans Affairs and other smaller agencies under the Governor's Office.

These, along with other items noted in Table 3.1, lead to the first recommendation. (The responses to the recommendations by the Finance and Administration Cabinet and Personnel Cabinet are in Appendices D and E, respectively.)

Recommendation 3.1

The task force on acceptable use should consider making the following additions or improvements to the Internet and e-mail acceptable use policy and all related policies

- **describe the range of consequences for violations;**
- **describe or reference the basic investigative process and state whether the results will be kept confidential;**
- **explicitly prohibit downloading e-mail from personal e-mail services;**
- **describe all aspects of handling confidential information, including secure storage and secure transmission;**
- **define procedures to secure private information contained in system logs;**
- **require employees to follow all computer safety and security practices;**
- **mention that the Commonwealth has the right to recover any costs of inappropriate employee computer use;**
- **require all employees to receive training on the acceptable use policy and related policies, including a thorough explanation of the need for the policies and procedures;**

- **specify a minimum retention period for system logs, even if the logs are to be discarded daily, and require each agency creating such logs to adopt its own standard;**
- **change the phrase "executive cabinets" to include all executive agencies; and**
- **direct all agencies to specify a minimum retention period for personal and transient e-mail records.**

Program Review staff and officials at the Personnel Cabinet had some concerns about how acceptable use policies might be applied to persons who are not classified employees. Table 3.1 lists categories of users that should be considered.

Recommendation 3.2

The task force on acceptable use should review the applicability of acceptable use policies to all possible users of executive branch computer resources. If any type of user appears not to be covered, the task force should take steps to ensure that the policies can be applied.

Some Implementation Procedures Could Be Improved

Although the Personnel Cabinet recognizes the importance of managing acceptable use, each agency has its own personnel office with considerable autonomy. Program Review staff found that agencies place different priorities on managing acceptable use and have different approaches. Thus, the recommendation on this matter is broad and will not apply in its entirety to all agencies.

There are several purposes for implementing an acceptable use policy. These include maintaining

- a good reputation and avoiding loss of goodwill,
- good productivity and avoiding wasted work time,
- efficient use of equipment and avoiding purchase of unneeded capacity,
- the integrity of the workplace and avoiding legal liability, and
- the security of computer systems and avoiding losses from cyber attacks.

In order to realize significant cost savings, it is necessary to enlist supervisors and employees.

Failure in any of these areas can be expensive and potentially embarrassing. It was not possible to get a firm estimate of the dollar value in most of these areas, but savings in the tens of millions of dollars per year seem possible. Some portion of those savings can come through the use of information technology, but

much of the benefit must come through the cooperation of supervisors and employees.

Additional funding, if needed, should be justifiable based on anticipated savings.

Some of these recommendations may require additional funds. Agencies should consider ways to justify startup funding in anticipation of future savings that would lead to a return on the investment.

Recommendation 3.3

The Personnel Cabinet and the personnel staff of each agency should implement an ongoing process to establish and promote a corporate culture of proper use of Commonwealth computer resources. The agencies should consider including

- **prevention of inappropriate use, beginning with the hiring process;**
- **developing an employee education program that explains the reasons for and benefits of acceptable computer use;**
- **training supervisors to notice personal problems that might lead to inappropriate use and to take corrective action;**
- **involving employees in the development of acceptable use policies and procedures;**
- **having procedures for employees to provide feedback and to report violations;**
- **training supervisors to build a culture that creates loyalty, dedication, and motivation;**
- **ensuring that policies and procedures are implemented and enforced uniformly within administrative units;**
- **giving regular feedback to employees on the level and cost of misuse in their department or division over time;**
- **giving regular feedback to employees on their own patterns of computer use;**
- **requiring employees to receive ongoing training on their role in computer system security;**
- **ensuring that every employee has access to a responsive computer assistance and problem-reporting process;**
- **considering adoption of an open office or visible monitor policy; and**
- **considering elimination of Web access on workstations that do not require it.**

The Kentucky Employee Handbook is an important tool for informing employees about policies and procedures. The current version of the handbook includes an outdated version of the acceptable use policy. The handbook also states that “no personal use is permitted.” This is inaccurate and should be corrected.

Recommendation 3.4

The Personnel Cabinet should assure that the Kentucky Employee Handbook section related to use of information technology resources is always as accurate and understandable to employees as possible.

To handle other costs related to file system capacity, local network capacity, and local security, each agency will need to implement its own tools and procedures. Staff found considerable variation among agencies in their approach to these issues.

Recommendation 3.5

To manage file storage, local network capacity, and workstation security, the Commonwealth Office of Technology and the information technology office of each agency should consider

- **implementing storage resource management or similar tools to limit the types and sizes of files that can be transmitted on the local network and stored on file servers and, to the extent possible, on workstations;**
- **using file access controls to restrict users to files and storage locations that are appropriate for their work;**
- **using file access controls, encryption, and other techniques to protect confidential or sensitive information;**
- **maintaining up-to-date and patched operating software and antivirus software on all workstations and servers;**
- **setting all workstations to lock if unused after 10 to 15 minutes and to require a password to reactivate; and**
- **limiting user permissions for workstations to prevent users from installing software or hardware or changing any sensitive system settings.**

Policy and Implementation Should Be Consistent Regarding Incidental Use

It appears that incidental Internet use is severely limited in practice. If this is the intent, then policy should clearly state it. If not, different limits should be set.

Although the acceptable use policy specifically allows incidental use of the Internet and e-mail, the Finance and Administration Cabinet has stated that its CSM rules will block all Internet sites that are not work related, unless an agency director requests otherwise. This block-first strategy conflicts with a core premise of CIO-060 ("Agencies may choose to add to this policy, in order to enforce more restrictive policies…"), rendering incidental Web use meaningless for many users.

Chapter 2 described a strategy used by the Department of Criminal Justice Training to manage incidental Internet use. Staff encourage the Finance and Administration Cabinet to explore this and other alternate ways to manage incidental Web use.

Recommendation 3.6

The Finance and Administration Cabinet should consider allowing access to non-work-related Internet sites that are appropriate for personal use, consistent with the overall philosophy of CIO-060. If such use is allowed, it should be in the context of good supervisory practice at the agency level.

Incidental use policies can differ for e-mail, the Internet, and the computer workstation. The cabinet's approach clearly indicates different treatment for e-mail and the Internet. To the extent that the filtering rules differ for them, it would be advisable for the task force on acceptable use to write a separate policy section for each.

Measurement and Evaluation of Outcomes Are Essential

Neither the Personnel Cabinet nor the Commonwealth Office of Technology maintains adequate information to judge the results of the acceptable use policy. The same is true for most state agencies. Measurements need to be made and compared over time in order to track the success of acceptable use management.

Recommendation 3.7

The Personnel Cabinet should design outcome measures to determine the effectiveness of acceptable use management on employee knowledge and behavior, including employee knowledge and support of the policies and inappropriate use incidents and their disposition. All agencies should be required to apply these measures at least annually and to report the results to the Personnel Cabinet. The Personnel Cabinet should compile the results and make them available for review.

Much of the information necessary to measure the performance of information technology is available in the detailed system logs of Internet access and e-mail transactions. Although it is technologically feasible to retain these logs indefinitely, it is difficult and unnecessary. For example, COT could take random or regular samples of the information or could keep data summaries instead of the original logs.

Recommendation 3.8

In addition to bandwidth use, the Commonwealth Office of Technology should retain adequate information about Web access and e-mail use to track important factors over time. This information should be archived for several years for comparison. The Commonwealth Office of Technology should consider providing breakdowns by such categories as day of week, period of time (work hours, evenings, weekend days), and category of Web site, as well as by agency (at the department or division level or lower).

Program Review staff identified three distinct types of testing that should be conducted to verify the security and operation of computer systems. Existing policies appear incomplete or do not apply to all agencies. Some of this testing could be expensive, but the cost should be justifiable based on future savings.

Recommendation 3.9

The Commonwealth Office of Technology should

- **increase the frequency of required vulnerability testing for agencies and expand its scope to include all systems—not just critical systems. Specifications should include tests of employee alertness and responsiveness to cyber attacks and especially to social engineering espionage.**
- **conduct periodic tests of the content security management system. These tests should determine whether a user can bypass the rules to gain access to prohibited Web sites or to send or receive prohibited types of e-mail.**
- **conduct periodic stress tests of the content security management system, as well as other protective systems, to ensure that they work properly under high-traffic conditions, such as when capacity has been exceeded.**

Outcome measurements are useless unless they affect the procedures that they measured. If changes are indicated, someone must be responsible for making them. Further, the law and technology of computer systems change rapidly. Some agencies told staff that they review technological changes quarterly. Many of the enterprise standards have an annual review cycle. Experts in the field concur that policies and procedures must be reviewed frequently to ensure that they are working, that they comply with the law, and that they most effectively utilize technology.

Recommendation 3.10

The Personnel Cabinet and the Finance and Administration Cabinet should review acceptable use policies and procedures at least annually. The review should ensure that they work properly, that they comply with the law, and that they use technology effectively. The review could be undertaken through a task force that includes representatives from these cabinets.

A Permanent High-level, Multi-agency Team Is Needed

Regular reassessment of policies and procedures is necessary to keep them up to date with rapidly changing laws and technology.

Best practice indicates that acceptable use policies need continual review and high-level management commitment. Accordingly, some person or entity should have oversight of all aspects of acceptable computer use for the state and ensure it remains a priority. Because acceptable use management requires human resource, information technology, and legal skills and resources, a multi-agency team is indicated. The current task force on acceptable use appears to meet these criteria.

Recommendation 3.11

The Personnel Cabinet, Finance and Administration Cabinet, and Office of the Governor should formalize the task force on acceptable use as a permanent entity with responsibility to review all policies and procedures related to acceptable computer use on a regular basis, oversee their management, and communicate their status to the governor and to executives in all agencies.

Works Cited

ABC News. "Harassment in the Supermarket." *ABCNews.com.* June 20, 2002. <http://abcnews.go.com/sections/primetime/DailyNews/primetime_ralphs_020620.html> (accessed Aug. 30, 2004).

Allen, Julia H., Edward F. Mikoski, Jr., Kevin M. Nixon, and Donald L. Skillman. *Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*. Arlington, VA: Internet Security Alliance, Carnegie Mellon University, 2002. <http://www.isalliance.org/news/BestPractices.pdf> (accessed July 28, 2004).

Allred, Stephen. "Employee Privacy and Workplace Searches." *Popular Government* 67.3 (Spring 2002): 33-35. <http://ncinfo.iog.unc.edu/pubs/electronicversions/pg/pgspr02/article5.pdf> (accessed Aug. 24, 2004).

American Management Association and ePolicy Institute. *2004 Workplace E-Mail and Instant Messaging Survey Summary*. < http://epolicyinstitute.com/survey/survey04.pdf> (accessed July 26, 2004).

BBC News. "Civil servants in net porn probe." *BBC News Online*, UK Edition. Aug. 26, 2004. <http://news.bbc.co.uk/1/hi/uk_politics/3600686.stm> (accessed Aug. 30, 2004).

Bennett, Margaret. "Employees Pass Buck on Security." *PC Magazine (UK)*. Feb. 16, 2004. <http://www.pcmag.co.uk/news/1152809> (accessed Aug. 23, 2004)

Blaky v. Continental Airlines. 751 A.2d 538 (NJ 2000).

Brick, Matthew. "Acceptable Internet & E-mail Use Policies." Central Iowa Chapter Society for Human Resource Management. <http://www.cishrm.org/Legal%20Updates/acceptable_internet_use.htm> (accessed Aug. 24, 2004).

Chiang, Harriet. "Chevron settles harass suit. 4 Bay Area women share $2.2 million." *San Francisco Chronicle* February 22, 1995: A1. <http://www.lexisnexis.com> (accessed Aug. 16, 2004).

Commonwealth of Kentucky. Commonwealth Office of Technology. Office of the Chief Information Officer. Policy CIO-060 "Internet and Electronic Mail Acceptable Use Policy." 2004.

---. Governor's Office for Technology. "Content Security Management (CSM) Executive Briefing." 2003.

Commonwealth of Virginia. Auditor of Public Accounts. *Impact Assessment for the 'ILOVEYOU' Computer Virus*. June 12, 2000. <http://jlarc.state.va.us/meetings/june00/apabrief.pdf> (accessed Aug. 11, 2004).

Cooper, Al, Gale H. Golden, and Jay Kent-Ferraro. "Online Sexual Behaviors in the Workplace: How Can Human Resource Departments and Employee Assistance Programs Respond Effectively?" *Sexual Addiction and Compulsivity* 9 (2002): 149-165.

D'Agostino, Debra. "Social Engineering for Security." *CIO Insight*. Aug. 22, 2003. <http://www.cioinsight.com/article2/0,1397,1228942,00.asp> (accessed Aug. 13, 2004).

Elliott, Rob. Transportation Cabinet Office of Inspector General. Staff Assistant. *Investigative Summary and Conclusions: Status Report OIG Case 2003-OIG-046*. May 25, 2004.

Fallows, Deborah. *Email at Work*. Washington, DC: Pew Internet and American Life Project. Dec. 8, 2002. < http://www.pewinternet.org/pdfs/PIP_Work_Email_Report.pdf> (accessed June 28, 2004).

Ferrarini, Elizabeth M. "Fighting the Network Storage Flood." *Computerworld* April 17, 2000. < http://www.computerworld.com/industrytopics/retail/story/0,10801,44460,00.html> (accessed Aug. 11, 2004).

Hayes, David L. "Copyright Liability of Online Service Providers." *Computer and Internet Lawyer* 19.10 (Oct. 2002).

Kelly, Chip (Systems and Information Security Manager, SAS Institute). Personal interview. July 8, 2004.

Kopelman, Richard E. "Managing for Productivity: One-Third of the Job." *National Productivity Review* 17.3 (Summer 1998): 1-2.

Leventhal v. Knapek. 266 F.3d 64 (2nd Cir. 2001).

Loftus, Tom. "Kentucky Punishes Workers Over Porn." Louisville *Courier-Journal* April 24, 2004.

Loney, Matt. "Your worst security threat: Employees?" ZDNet UK. April 23, 2002. <http://news.zdnet.co.uk/business/management/0,39020654,2108940,00.htm> (accessed Aug. 23, 2004).

Lyon, Christine, and Miriam Wugmeister. "The Most Overlooked Component of Data Security: Your Employees." Mondaq's Article Service. July 20, 2004. <http://www.mondaq.com/article.asp?articleid=27397> (accessed Aug. 13, 2004).

Meloff v. The New York Life Insurance Company. 1999 WL 604871 (S.D. NY 1999).

Mooney, Matthew L. “Legal Considerations in Internet Access and Email Use by Employees.” Mooney, Mooney, and Mooney, Lexington, KY (Nov. 7, 2003).

Moorman, Robert H., and Deborah L. Wells. “Can Electronic Performance Monitoring Be Fair? Exploring Relationships Among Monitoring Characteristics, Perceived Fairness, and Job Performance.” *Journal of Leadership and Organizational Studies* 10.2 (2003): 2-16.

Morrow v. Morrow, Inc. 911 P.2d 964 (OR Ct. App. 1996).

Muhl, Charles J. “Workplace e-mail and Internet use: Employees and employers beware.” *Monthly Labor Review* 126.2 (Feb. 2003): 36-45. <http://stats.bls.gov/opub/mlr/2003/02/art3full.pdf> (accessed July 13, 2004).

Mullich, Joe. “Cracking the Ex-Files.” *Workforce Management* (Sept. 2003): 51-54.

National Association of State Chief Information Officers. “Information Privacy: A Spotlight on Key Issues.” Feb. 2004, Version 1.0. <https://www.nascio.org/membersOnly/documents/InformationPrivacy2004.pdf> (accessed June 28, 2004).

Niehoff, Brian P., and Robert J. Paul. “Causes of Employee Theft and Strategies that HR Managers Can Use for Prevention.” *Human Resource Management* 39.1 (2000): 51-64

O'Connor v. Ortega. 480 U.S. 709 (1987).

Oliphant, Becky J., and Gary C. Oliphant. “Using a Behavior-Based Method to Identify and Reduce Employee Theft.” *International Journal of Retail and Distribution Management* 29.10 (2001): 442-451.

Parvaz, D. “E-mail abuse firings called unfair. Worst offenders kept jobs, say some of those disciplined.” *The Seattle Post-Intelligencer*. July 17, 2002: A1. <http://infoweb.newsbank.com> (accessed Aug. 16, 2004).

Peck, Kimberley T., and Amy J. McKee. “Sexual Addiction and the Workplace: A Public Sector Employer’s Response.” *Sexual Addiction and Compulsivity* 9 (2002): 127-138.

SANS Institute. “InfoSec Acceptable Use Policy.” SANS Institute Security Policy Project. <http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf> (accessed July 28, 2004).

Savage, Marcia. “Former Hacker Mitnick Details the Threat of ‘Social Engineering.’” *Computer Reseller News*. April 28, 2003. <http://www.crn.com/showArticle.jhtml?articleID=18830074&flatPage=true> (accessed Aug. 13, 2004)

Shipley, David. “Liability Issues Facing Online Businesses.” *Arkansas Lawyer* 36.1 (Winter 2001): 20-26. <http://www.arkbar.com/Ark_Lawyer_Mag/Winter%202001/pg20_liab_issues_onlinebu.htm> (accessed Aug. 24, 2004).

Solomon, Melissa. "Calculating Productivity Losses." *Computerworld* July 8, 2002: <http://www.computerworld.com/careertopics/careers/labor/story/0,10801,72483,00.html> ("Quick link" #31118 accessed Aug. 9, 2004).

Stone, Brad. "Is the Boss Watching? Online: Call it Orwellian or a model for productivity, but software that allows companies to monitor their employees' Web surfing is a burgeoning business." *Newsweek* Sept. 30, 2002: 38.

State of Texas. Department of Information Resources. "Personal Use of E-Mail & Internet Services." SRRPUB04. July 30, 2002. <http://www.dir.state.tx.us/standards/srrpub04.htm> (accessed Aug. 6, 2004).

Symantec® Security Response Glossary. <http://securityresponse.symantec.com/avcenter/glossary/index.html> (accessed Aug. 30, 2004).

Thomas, Ralph, and Andrew Garber. "Department of Lust and Indecency? State L&I workers fired for racy e-mails." *The Seattle Times*. April 25, 2002: A1. <http://infoweb.newsbank.com> (accessed Aug. 16, 2004).

United States. Department of the Treasury. Inspector General for Tax Administration. *Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data*. June 2003. (Reference Number 2003-20-133.) <http://www.ustreas.gov/tigta/2003reports/200320133fr.pdf> (accessed Aug. 10, 2004).

---. General Accounting Office. *Employee Privacy: Computer-Use Monitoring Practices and Policies of Selected Companies*. Publication GAO-02-717. Sept. 2002. http://www.gao.gov/new.items/d02717.pdf (accessed Feb. 18, 2004).

---. General Services Administration. Federal CIO Council. "Recommended Executive Branch Model Policy/Guidance on 'Limited Personal Use' of Government Office Equipment Including Information Technology." May 19, 1999. <http://www.cio.gov/archive/limited_personaluse_memo_policy.pdf> (accessed July 29, 2004).

---. National Center for Education Statistics. *Weaving a Secure Web Around Education: A Guide to Technology Standards and Security*. April 2003. <http://nces.ed.gov/pubs2003/2003381.pdf > (accessed July 12, 2004).

Urbaczewski, Andrew, and Leonard M. Jessup. "Web Browser, What's That Secret You're Keeping?" *Business Horizons* 46:5 (Sept./Oct. 2003): 25-32.

Weaver, Nicholas, and Vern Paxson. *A Worst-Case Worm*. May 5, 2004. <http://www.dtc.umn.edu/weis2004/weaver.pdf> (accessed Aug. 10, 2004).

Websense, Inc. *Desktop or Online – Employee Game Use is Growing Problem*. March 26, 2003. < http://www.websense.com/company/news/pr/Display.php?Release=03032653> (accessed Aug. 9, 2004).

Websense, Inc. *Web@Work Survey Results 2004*. 2004. <http://www.websense.com/company/news/research/webatwork2004.pdf> (accessed Aug. 24, 2004)

Wikipedia™ Online Encyclopedia. <http://en.wikipedia.org/wiki/Main_Page> (accessed Aug. 30, 2004).

Zimmerman, Eilene. "HR Must Know When Employee Surveillance Crosses the Line." *Workforce.* Feb. 2002: 38-45. <http://www.workforce.com/archive/feature/23/16/50/index.php> (accessed Aug. 24, 2004).

Appendix A

Issues for Further Study

Program Review staff identified five questions related to acceptable computer use that were outside the scope of the study but that may merit consideration.

1. What are other risks and costs?

Wards of the State. What risks or costs might the Commonwealth incur from the actions of wards of the state other than correctional inmates? If state government might be liable for their actions, then the agencies that manage their computer use should take special care to ensure acceptable use. Loss of goodwill, capacity costs, and security risks should also be studied. Examples include patients at state-run mental hospitals, children in foster care or residential care, and mentally ill or mentally retarded adults in residential care or training institutions.

Branches of Government. The Kentucky taxpayer incurs risks and costs from the actions of employees in all branches of state government. It would be prudent for all agencies in all branches to implement best practices to manage appropriate computer use. Is it feasible and desirable for Kentucky to adopt a government-wide acceptable use policy and enforcement mechanism similar to those in Tennessee or Delaware?

State-supported Institutions. What risks or costs does the Kentucky taxpayer incur from the actions of those who are not state employees but who work for entities that receive state funds? Because taxpayer dollars support these institutions, their ability to manage acceptable computer use should be of interest to state government. Examples of such entities include higher education, school systems, and Kentucky Retirement Systems.

Users of the Kentucky Information Highway. What risks or costs might the Commonwealth incur for actions of subscribers of the Kentucky Information Highway that are not affiliated with state government, such as libraries and local governments? As an Internet service provider, the Commonwealth Office of Technology might incur some legal liability and certainly faces risks such as loss of goodwill, capacity cost, and security failures.

2. What are the advantages and disadvantages of keeping detailed historical data to support investigations?

When a violation of acceptable use policy is brought to the attention of management, the personnel and legal staff must investigate and gather evidence. The investigation must show an unmistakable pattern of inappropriate use. Often, this means monitoring the employee's Web use, e-mail, and workstation logs over a period of time to build the case.

Cyber attacks, particularly the kind found at the Transportation Cabinet, often occur over a period of time. When an undetected cyber attack occurs, much of the information needed to trace it is contained in logs of Web use, local network traffic, and workstation activity.

Internet gateway computers keep detailed Internet access logs and other audit trails of every Web page request and e-mail message. These are the same logs required to investigate cyber attacks and violations of acceptable use. Some organizations, including the Commonwealth Office of Technology, delete them daily. This means that investigations can only collect data after the violation has come to light. Security investigations are hampered by the lack of an evidence trail to follow.

Other organizations keep detailed Internet access logs and other audit trails for a longer period of time, some of them indefinitely. This allows investigators to look at the history of an alleged violator and build a case without depending on future misbehavior. Security investigations can more easily determine how an attack occurred and how extensive the damage may be.

However, the decision to keep these audit trails is not clear-cut. Keeping them may create issues of privacy versus open records or evidentiary discovery requests. It could expose the Commonwealth to some liability. Further, there is the practical question of how to save the audit trails, which require a considerable amount of storage.

3. Should employees reimburse state government for personal use of computers?

Several states have looked at ways to charge employees for personal use of computing resources. This is similar in concept to billing for telephone usage. However, there are considerable technical obstacles. It also raises the question of ownership; employees who pay for using the resources might then feel some ownership or entitlement to use them.

4. Should state government maintain an inventory of computer software and hardware?

For planning purposes, as well as to ensure proper licensing, it might be helpful for the Commonwealth of Technology to compile inventories of computer software and hardware from all agencies. Costs and benefits of this should be considered.

5. Can removing e-mail addresses from Web pages reduce spam?

An industry best practice for reducing spam is to remove e-mail addresses from Web pages. Spam purveyors have software tools that scan Web pages and harvest e-mail addresses, which then become spam targets. By removing addresses from Kentucky government Web pages, this harvesting could be reduced. To provide the public with an alternate way to contact government workers, Kentucky.gov Web sites could include a message form that accepts messages for agency personnel.

Appendix B

Research Methods

In conducting the study of acceptable computer use, staff interviewed officials with the following Kentucky agencies:

- Commonwealth Office of Technology (formerly Governor's Office for Technology),
- Department of Corrections,
- Department of Criminal Justice Training,
- Environmental and Public Protection Cabinet,
- Personnel Cabinet, and
- Transportation Cabinet.

Staff also obtained written responses on the following Kentucky agencies' human resource and information technology practices in managing computer use:

- Commerce Cabinet,
- Economic Development Cabinet,
- Education Cabinet,
- Finance and Administration Cabinet,
- Health and Family Services Cabinet,
- Justice and Public Safety Cabinet,
- Department of Military Affairs, and
- Department of Veterans Affairs.

For comparison, staff obtained acceptable use policies and/or interviewed officials of the following states and organizations:

- Arkansas;
- Connecticut;
- Delaware;
- Kansas;
- Michigan;
- Minnesota;
- Montana;
- Nevada;
- North Carolina;
- Ohio;
- Pennsylvania;
- Tennessee;
- Texas;
- Utah;
- Wisconsin (Department of Administration);
- U.S. Department of Veterans Affairs;
- U.S. Office of Personnel Management;
- Flathead Valley (Montana) Community College;
- Indiana University;
- University of Kentucky;
- University of Louisville;
- Ashland, Inc.;
- SAS Institute, Inc.; and
- United Parcel Service, Inc.

Staff conducted a literature review to develop best practice guidelines for human resource and information technology approaches to managing acceptable computer use. Staff also conducted legal research to assess the legal risks of computer use.

To gather information on the level of violations of acceptable use policy in Kentucky, staff polled all major agencies for information on the number of employees, the number disciplined overall, and the number disciplined for such violations over the past four fiscal years. The following agencies provided this information:

- Commerce Cabinet,
- Economic Development Cabinet,
- Education Cabinet,
- Environmental and Public Protection Cabinet,
- Finance and Administration Cabinet,
- Health and Family Services Cabinet,
- Justice and Public Safety Cabinet,
- Department of Military Affairs,
- Personnel Cabinet,
- Transportation Cabinet, and
- Department of Veterans Affairs.

The table below gives the totals and percentages for this period of time, with and without the Transportation Cabinet. Figure 3.A is based on this table.

Number and Percent of Employees Disciplined
FY 2001 to FY 2004

			All Disciplinary Actions		Violations of Acceptable Use Policy	
	Fiscal Year	**Total State Employees**	**Employees Disciplined**	**As % of All Employees**	**Employees Disciplined**	**As % of All Employees**
With Transportation Cabinet	2001	36,122	680	1.88%	59	0.16%
	2002	36,764	756	2.10%	36	0.10%
	2003	36,700	800	2.18%	49	0.13%
	2004	34,345	739	2.15%	85	0.25%
Without Transportation Cabinet	2001	29,927	464	1.55%	46	0.15%
	2002	30,597	524	1.71%	32	0.10%
	2003	30,951	612	1.98%	42	0.14%
	2004	29,156	515	1.77%	37	0.13%

Appendix C

This appendix consists of six policy documents from the Commonwealth Office of Technology:

Office of the Chief Information Officer

ENTERPRISE POLICY

Policy Number: CIO-060 **Effective Date:** 05/15/96

Revision Date: 04/22/04

Subject: Internet and Electronic Mail Acceptable Use Policy

Policy Statement: The purpose of this enterprise policy is to define and outline acceptable use of Internet and Electronic mail (E-mail) resources in state government. These rules and guidelines are in place to protect both the user and the Commonwealth. This policy requires all agencies and employees and other users to comply with the acceptable use provisions.

Policy Maintenance: The Department of Personnel, the Governor's Office for Technology (GOT) Office of Infrastructure Services, and the GOT Office of Policy and Customer Relations share responsibility for maintenance and interpretation of this policy. Agencies may choose to add to this policy, in order to enforce more restrictive policies as appropriate and necessary. Therefore, employees are to refer to their agency's internal acceptable use policy, which may have additional information or clarification of this enterprise policy.

Applicability: This policy is to be adhered to by all Executive Branch agencies and users, including employees, contractors, consultants, temporaries, volunteers and other workers within state government. This policy applies to all resources and information technology equipment owned or leased by the Commonwealth regardless of the time of day, location or method of access.

Responsibility for Compliance: Each agency is responsible for assuring that employees and users under their authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that intentional, inappropriate use of Internet and E-mail resources may result in disciplinary action

pursuant to KRS 18A up to and including dismissal. To demonstrate awareness and knowledge of this policy, signed acknowledgement forms are required. It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for GOT's efforts to remedy inappropriate usage.

Policy: As provisioned, Internet and E-mail resources, services and accounts are the property of the Commonwealth of Kentucky. These resources are to be used for state business purposes in serving the interests of state government, citizens and customers in the course of normal business operations. This Acceptable Use Policy represents a set of rules and guidelines to be followed when using the Kentucky Information Highway (KIH) or any other network that is used as a result of its KIH connection, including Internet and E-mail.

In compliance with the laws of the Commonwealth and this policy, employees of the Commonwealth of Kentucky are encouraged to use the Internet and E-mail to their fullest potential to:

- Further the State's mission
- To provide service of the highest quality to its citizens
- To discover new ways to use resources to enhance service, and
- To promote staff development

State employees should use the Internet and E-mail, when appropriate, to accomplish job responsibilities more effectively and to enrich their performance skills.

The acceptable use of Internet and E-mail represents the proper management of a state business resource. The ability to connect with a specific Internet site does not in itself imply that an employee is permitted to visit that site. Monitoring tools are in place to monitor employees' use of E-mail and the Internet. Employees shall have no expectation of privacy associated with E-mail transmissions and the information they publish, store or access on the Internet using the Commonwealth's resources.

Incidental personal uses of Internet and E-mail resources are permissible, but not encouraged. Excessive personal use shall lead to loss of the resource privileges and may result in disciplinary action pursuant to KRS 18.A up to and including dismissal. Employees are responsible for exercising good judgment regarding incidental personal use. Any incidental personal use of Internet or E-mail resources must adhere to the following limitations:

- It must not cause any additional expense to the Commonwealth or the employee's agency
- It must be infrequent and brief
- It must not have any negative impact on the employee's overall productivity
- It must not interfere with the normal operation of the employee's agency or work unit

- It must not compromise the employee's agency or the Commonwealth in any way
- It must be ethical and responsible

Employee/User Responsibilities:

- Read, acknowledge and sign an agency acceptable use policy statement before using these resources.

- Use access to the Internet and E-mail in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulation.

- As with other forms of publications, copyright restrictions/regulations must be observed.

    - Employees shall be aware that their conduct or information they publish could reflect on the reputation of the Commonwealth. Therefore, professionalism in all communications is of the utmost importance.

    - Employees that choose to use E-mail to transmit sensitive or confidential information should encrypt such communications using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services.

    - Employees shall represent themselves, their agency or any other state agency accurately and honestly through electronic information or service content.

Supervisor Responsibilities:

- Supervisors are required to identify Internet and E-mail training needs and resources, to encourage use of the Internet and E-mail to improve job performance, to support staff attendance at training sessions, and to permit use of official time for maintaining skills, as appropriate.

- Supervisors are expected to work with employees to determine the appropriateness of using the Internet and E-mail for professional activities and career development, while ensuring that employees do not violate the general provisions of this policy, which prohibit using the Internet and E-mail for personal gain.

- Managers and supervisors who suspect that an employee is using E-mail inappropriately must follow GOT's standard written procedure for gaining access to the employee's E-mail account.

Agency Responsibilities:

- E-mail and Internet access should be used for “appropriate business use" only. Incidental personal use is permissible, but not encouraged. This policy recognizes the specific definition of appropriate business use may differ among agencies based on their mission and functions. Therefore, each agency should define appropriate business use and make certain employees and users are fully informed.

- Create an Internet and E-mail Acceptable Use Policy statement and require a signed acknowledgement by all employees and users before accessing these resources.

- Agencies that permit the use of E-mail to transmit sensitive or confidential information should be aware of the potential risks of sending unsecured transmissions. E-mail of this nature should, at a minimum, contain a confidentiality statement. E-mail content and file attachments considered highly sensitive or confidential must be encrypted using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services. To protect confidential data, some federal laws require the use of encrypted transmission to ensure regulatory compliance.

- Agencies are responsible for the content of their published information and for the actions of their employees, including the proper retention and disposal of E-mail records. Enterprise Standard 4060: Recordkeeping – Electronic Mail should be observed.

- Any commercial use of Internet connections by agencies must be approved by GOT to make certain it does not violate the terms of GOT's agreement with the Commonwealth’s Internet provider. No reselling of access is allowed.

- Agencies shall not accept commercial advertising or vendor-hosted website advertising for which the agency receives compensation. As a general practice, state agencies should avoid endorsing or promoting a specific product or company from agency websites, however the placement of acknowledgements, accessibility and certification logos are acceptable.

Prohibited and Unacceptable Uses: Use of Internet and E-mail resources is a privilege that may be revoked at any time for unacceptable use or inappropriate conduct. Any abuse of acceptable use policies may result in notification of agency management, revocation of access and disciplinary action up to and including dismissal. The following activities are, in general**, strictly prohibited**. With the proper exception approved, employees may be exempt from these prohibitions during the course of job responsibilities and legitimate state government business.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including but not limited to, the
- downloading, installation or distribution of pirated software, digital music and video files.

- Engaging in illegal activities or using the Internet or E-mail for any illegal purposes, including initiating or receiving communications that violate any state, federal or local laws and regulations, including KRS 434.840-434.860 (Unlawful Access to a Computer) and KRS 512.020 (Criminal Damage to Property Law). This includes malicious use, spreading of viruses, and hacking. Hacking means gaining or attempting to gain the unauthorized access to any computers, computer networks, databases, data or electronically stored information.

- Using the Internet and E-mail for personal business activities in a commercial manner such as buying or selling of commodities or services with a profit motive.

- Using resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, whether through language, frequency or size of messages. This includes statements, language, images, E-mail signatures or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

- Using abusive or objectionable language in either public or private messages.

- Knowingly accessing pornographic sites on the Internet and disseminating, soliciting or storing sexually oriented messages or images.

- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or E-mail. This includes the use of false or misleading subject headers and presentation of information in the distribution of E-mail.

- Employees are not permitted to use the E-mail account of another employee without receiving written authorization or delegated permission to do so.

- Employees are not permitted to forge E-mail headers to make it appear as though an E-mail came from someone else.

- Sending or forwarding chain letters or other pyramid schemes of any type.

- Sending or forwarding unsolicited commercial E-mail (spam) including jokes.

- Soliciting money for religious or political causes, advocating religious or political opinions and endorsing political candidates.

- Making fraudulent offers of products, items, or services originating from any Commonwealth account.

- Using official resources to distribute personal information that constitutes an unwarranted invasion of personal privacy as defined in the Kentucky Open Records Act, KRS 61.870.

- Online investing, stock trading and auction services such as eBay unless the activity is for Commonwealth business.

- Developing or maintaining a personal web page on or from a Commonwealth device.

- Use of peer-to-peer (referred to as P2P) networks such as Napster, Kazaa, Gnutella, Grokster, Limewire and similar services.

- Any other non-business related activities that will cause congestion, disruption of networks or systems including, but not limited to, Internet games, online gaming, unnecessary Listserve subscriptions and E-mail attachments. Chat rooms and messaging services such as Internet Relay Chat (IRC), I SeeK You (ICQ), AOL Instant Messenger, MSN Messenger and similar Internet-based collaborative services.

References:

Enterprise Standard 2600: Electronic Mail and Messaging –
http://www.gotsource.ky.gov/dscgi/ds.py/Get/File-9360/2600_-_Electronic_Mail_-Messaging.doc

Enterprise Standard 4600: Recordkeeping – Electronic Mail –
http://gotsource.ky.gov/dscgi/ds.py/Get/File-20485/Standard_4060_Electronic_Mail.doc

KRS 434.840-434.860, Unlawful Access to a Computer
http://www.lrc.state.ky.us/KRS/434-00/840.PDF

State Government Employee Handbook
http://kygovnet.state.ky.us/personnel/emphand.htm

Office of the Chief Information Officer
ENTERPRISE POLICY/PROCEDURE

Policy Number: CIO-079 **Effective Date**: 04/01/04
Revision Date**:**

Subject: Logon Security Notice

Policy Statement: This policy is intended to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources, by requiring all logon screens include a security notice indicating that the system must be used for authorized purposes only. A security notice or banner is required when logging on to any device connected to the Kentucky Information Highway (KIH) or any network within the KIH. This policy supports the principles of the Enterprise Security Architecture as expressed in Enterprise Security Domain 5000.

Applicability: This policy is to be adhered to by all agencies and employees within the Executive Branch of state government.
Responsibility for Compliance: Each agency is responsible for assuring that employees within their organizational authority are aware of the provisions of this policy, that compliance by the employee is required, and that intentional, inappropriate use may result in disciplinary action pursuant to KRS 18A, up to and including dismissal.

It is also each Executive Cabinet's responsibility to enforce and manage this policy. Failure to comply will result in additional shared service charges to the agency for the Office for Technology's efforts to remedy intrusion activities resulting from unauthorized usage where insufficient security notice was not provided by the agency.

Policy Maintenance: The Governor's Office for Technology, Office of Infrastructure Services, has the responsibility for the maintenance of this policy. Agencies may choose to add to this policy as appropriate, in order to enforce more restrictive standards. Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

Policy: All logon screens must include a security notice that states the involved system may be used only for authorized purposes.

Specifically, the notice must state the following:

- Only authorized users may access the system.
- Users who access the system beyond the warning page represent that they are authorized to do so.
- Unauthorized system usage or abuse is prohibited and subject to criminal prosecution.
- System usage may be monitored and logged.

Security notices should not contain specific information about the organization, operating system, network configuration, or other internal information, thus making it more difficult for unauthorized users to exploit system vulnerabilities. In addition, the security notice should not include words that imply consent to use the computer system such as “greetings" or "welcome.”

Minimum Required Security Notice

Notice: This is a government computer system and is the property of the Commonwealth of Kentucky. It is for authorized use only regardless of time of day, location or method of access. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on the system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized state government and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such at the discretion of the Commonwealth of Kentucky. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By clicking “OK” you acknowledge your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

Office of the Chief Information Officer

ENTERPRISE POLICY/PROCEDURE

Policy Number: CIO-082 **Effective Date:** 5/15/04
Revision Date:

Subject: Critical Systems Vulnerability Assessments

Policy: The purpose of this policy is to establish procedures for network vulnerability assessments of the servers and operational environments of critical systems by state agencies utilizing the Kentucky Information Highway (KIH), hereinafter referred to as "Agency." The scanning and testing is only permitted to target the resources owned or managed by the Agency or managed through Enterprise Shared Services.

Agencies will be responsible for identifying critical systems based on the nature of the data and the system's business function or mission. The term "critical system" refers to the server, or servers, that support one or more critical business application. This may include web servers, database servers, and other servers that are essential to the operation of the business application. Each Agency shall engage a third party to assess all critical systems under the Agency's responsibility both upon initial implementation into production use and every two (2) years thereafter. These network and server vulnerability assessments do not include the development environments, or application software, related to these systems, which must be tested separately. Each agency shall follow the appropriate notification process outlined in this policy prior to conducting the assessments. It is the responsibility of the Agency, in consultation with the Cabinet CIO, to engage an Appropriate and Qualified Organization that is considered an external or third party entity to ensure objectivity and accuracy in the assessment. It is the responsibility of the Agency to ensure that the entity conducting the vulnerability assessment has signed an appropriate confidentially statement prohibiting the divulgence of sensitive information. This requirement may not apply to certain state or federal agencies, such as the Auditor of Public Accounts.

It is important that scanning and penetration testing activities are conducted in a manner that will not disrupt or otherwise degrade the quality of services that the Governor's Office for Technology (GOT) provides to agencies not involved in the assessment process. To this purpose, GOT will aggressively block any scans suspected to be causing any service disruption until this activity can be determined to be a part of an agency's authorized security assessment, after which, appropriate action will be taken to allow the assessment activity to continue.

Policy Maintenance: The Governor's Office for Technology, Office of Infrastructure Services, Division of Security Services has the responsibility for maintaining and updating this procedure. The revision review cycle for this procedure will be annually.

Responsibility for Compliance:
Each agency is responsible for assuring that appropriate employees within their organizational authority have been made aware of the provisions of this policy, that compliance by the employee is expected, and that the failure to comply with this policy may result in disciplinary action pursuant to KRS 18A up to and including dismissal.

It is also each Agency's responsibility to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for the Governor's Office for Technology's efforts to remediate issues related to the lack of adequate systems/network infrastructure security.

Definitions:
Application – A software program designed to perform a specific function.

Critical Systems – The servers and computing infrastructure that support an automated business process identified as critical by the Agency based on the nature of the information stored (sensitive/confidential), importance to the agency's mission, or as stipulated by statute or regulation.

Network Environment – Includes the communications hardware and software components that are utilized by the system to exchange information with internal or external users of the system. Includes technical configuration, maintenance procedures, and overall functional compliance with Commonwealth security policy.

Operational Environment - Includes server hardware and software components used to process, store, or backup/recover information on a critical system. Includes technical configuration, maintenance procedures, and overall functional compliance with Commonwealth security policy.

Penetration Testing – A security testing procedure to proactively identify computer system vulnerabilities in order to locate and identify any weaknesses that could be exploited by intruders.

Scanning – An automated process to query computer systems in order to obtain information on services that are running the level of security.

System – An automated business process that is operated on computer hardware and software and is connected to the network.

Appropriate and Qualified Organization – Any contract or government organization that is not a part of the Agency's organizational structure and has demonstrated the technical capability to conduct security assessments for government agencies. This may include state or federal auditing agencies, state approved security contract vendors, or other external organizations whose capabilities and experience can be determined sufficient to conduct these assessments.

Procedure: Vulnerability assessments to identify potential security vulnerabilities in an Agency's IT infrastructure are recommended and encouraged by the Governor's Office for Technology. However, prior notification of performing vulnerability scanning and/or penetration testing of KIH devices/infrastructure must be provided to the director of the Governor's Office for Technology's Division of Security Services (DSS) before such activity can commence.

A Vulnerability Assessment Notification form (GOT-F0XX) must be fully completed and submitted to the DSS director at least three (3) full business days prior to the assessment activities. The form must be signed by the Agency's CIO or designated executive management and submitted to the Governor's Office for Technology's Division of Security Services, 101 Cold Harbor Drive, Frankfort, KY 40601. The form may be emailed without signature to the DSS Director if an email originated by the Agency CIO or other designated executive management accompanies the form. Upon receipt of a completed Vulnerability Assessment Notification form, the Governor's Office for Technology will review the declared targets to ensure that they are not shared resources with any other agency.

If the Agency's vulnerability assessment activities are detected by GOT's security and intrusion detection systems, the offending device will be blocked. This may temporarily suspend the Agency's assessment activities, and could possibly affect Agency services. In this case, the Agency will be required to open a Help Desk ticket by contacting the Governor's Office for Technology's Help Desk at 502.564.7576. GOT will then unblock the activity in order for the assessment to resume.

If the assessment is to be scheduled after normal business hours, the Agency may request that GOT staff be onsite to restore any affected services. This request should be included on the GOT-F0XX form in the Additional Information section. Assessments performed after normal business hours without this specific support request may result in a significant delay to unblock devices, which were stopped by the Intrusion Detection System.

Upon receipt of the GOT-F0XX form, DSS will notify the contact person and CIO/Executive Management listed on the form via email as to the status of the request. Response time between DSS' receipt of the GOT-F0XX form and notification to the Agency should be no more than two (2) business days. The form will be assigned a tracking number and electronically stored in GOT Source along with associated correspondence. Appropriate GOT staff will be made aware of the scheduled vulnerability assessment in order to field any inquiries concerning this activity and to arrange after hours staff availability onsite if necessary.

Governor's Office for Technology

Vulnerability Assessment Notification

Cabinet/Agency: Request Date:

Contact Person: Telephone:

Organization/Vendor Conducting Assessment:

Date(s) and Time(s) of Scheduled Assessment/Scanning:

Type of Assessment/Scan:

Assessment/Scanning Tool Used:

Names & TCP/IP Addresses of Servers or Networks Being Scanned:

TCP/IP Addresses of Authorized Scanning Machines:

Description of Assessment/Additional Information:

Agency CIO Signature: _____ Date: _____

For OT Use Only

Schedule Accommodated: ____Yes ____ No Tracking Number: _____

DSS Director Signature: _____ Date: _____

Form Instructions:

A Vulnerability Assessment Notification form (GOT-F0XX) must be fully completed and submitted to the DSS director at least three (3) business days prior to any vulnerability assessment of the KIH infrastructure and/or any KIH device. The form must be signed by the Agency's CIO or designated executive management and submitted to the Governor's Office for Technology's Division of Security Services, 101 Cold Harbor Drive, Frankfort, KY 40601. The form may be emailed without signature to the DSS Director if an email originated by the Agency CIO or other designated executive management accompanies the form.

If the Agency's vulnerability assessment is detected by GOT's security systems and detection systems, the offending device will be blocked. This may temporarily suspend the Agency's assessment activities, and could possibly affect Agency services. In this case, the Agency will be required to open a Help Desk ticket by contacting the Governor's Office for Technology's Help Desk at 502.564.7576. GOT will then unblock the activity in order for the assessment to resume.

If the assessment is to be scheduled after normal business hours, the Agency may request that GOT staff be onsite to restore any affected services. This request should be included on GOT-F0XX form in the Additional Information section.

Any questions regarding this process should be directed to the DSS Director via email or by telephone at 502.564.7680.

Enterprise Standards:
3000 Network Domain

Category:
3550 Network Services – Storage Area Networks

Definition:
A network storage system that contains a disk or disk array for storing data and serves as a high-speed subnetwork of shared storage devices. A storage area network (SAN) handles storage management functions like archive/retrieval, backup/restore and disaster recovery. Generally a SAN utilizes a high-bandwidth fibre channel connection for high-speed transfer of data over longer distances, but may use a SCSI interface. Using fiber optic cable to connect storage devices, fibre channel supports full-duplex data transfer rates of 100 MBps. This storage architecture makes all storage devices available to all servers on a LAN or WAN.

Rationale:
It is recommended that all critical data be stored on storage devices or file servers rather than individual desktop workstations. Emerging applications are more storage-intensive and may require ready access to stored data on the network. Users are demanding increased service levels from their network, including online access to universal data stores. A SAN promotes storage consolidation and offers a modular storage solution that can grow with agency data storage needs. With a SAN network, any host on the network can access any storage device and it stored files without interfering with LAN traffic.

Approved Standard(s):

Approved Product(s):
None

Justification:
Using a SAN for network backup allows for fast, reliable backup and recovery of data. Fibre Channel SAN systems create a pool of RAID or tape storage that can be shared among multiple servers simultaneously. Isolated data sources can be interconnected and made generally available to multiple servers. This storage architecture provides improved availability and performance, while server power is directed to handling critical business applications.

Technical and Implementation Considerations:
In the near future, agencies may have the need to use a storage area network of shared storage devices instead of a discrete tape backup unit at each server. SAN technology is more complex, and is now more expensive in terms of initial acquisition cost, but offers the potential for more flexible and efficient management of enterprise storage resources.

Emerging Trends and Architectural Directions:
GOT is evaluating SAN solutions within the data center and will provide information and assistance to agencies regarding the experience with the systems deployed.

Review Cycle:
Annually

Timeline:
Revision date: May 1, 2001
Effective date: December 20, 1999

Enterprise Standards:
4000 Information/Data Domain

Category:
4060 Recordkeeping - Electronic Mail

Definition:
Electronic mail (email) messages are any communication supported by email systems for the conduct of official agency business internally, between other state, local, and federal agencies, and with constituents, voters, vendors, clients, citizens, and others. This definition applies equally to the contents of the communication, the transactional information associated with each message, and any attachments to the body of the message.

Electronic mail systems enable users to compose, transmit, receive, and manage, text and/or graphic electronic messages and images across LAN and WAN networks and through gateways connecting the latter with the Internet.

Rationale:
The email environment in Kentucky state government has a current transaction volume that exceeds eighty million messages a month. This figure dramatically illustrates the extent of agency use and reliance on email services to conduct state business. Two existing Enterprise policies, (1) Status of Electronic Mail as a Public Record, and (2) Internet and Electronic Mail Acceptable Use Policy, CIO-060, have emphasized that electronic mail is statutorily defined as a public record and set broad parameters for the management and acceptable use of email in the executive branch of state government. This standard clarifies agency responsibilities.

Approved Standard(s):
KRS sections 61.870 (Open Records) and 171.410 (State Archives and Records) define "public record" to mean all books, papers, maps, photographs, cards, tapes, disks, diskettes, records, and other documentation/documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency. Being public record under these terms, electronic mail must be managed to provide appropriate, reliable, and cost-effective evidence of the business activities it supports, relates to, or documents. Its integrity, completeness, retrievability, public accessibility, and retention all should respond to agency or Enterprise business requirements.

Agencies establish recordkeeping rules[1] that are appropriate to the business functions they normally perform. These rules reflect best recordkeeping practices associated with the specific business processes agencies are engaged in, as well as any explicit legal, audit, or archival requirements that have been established. Agencies must apply these recordkeeping rules to the administration of electronic mail as it relates to the same business functions.

[1] The Kentucky Department for Libraries and Archives and the State Archives and Records Commission have statutory authority to establish records management requirements for public agencies of the Commonwealth, and agency recordkeeping practice should conform to standards, schedules, or guidelines developed by them.

The following general requirements must be met by agencies in managing email:

The integrity, reliability, and authenticity of email messages must be protected through compliance with all security and data management requirements established in the Enterprise Architecture and Standards.

Per the acceptable use policy referenced above, agencies must instruct employees and take steps to ensure that non-business related email messages are regularly deleted from email stores (inboxes and personal folders). Transitory messages, which are defined as messages that are for informational and reference purposes only and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt, must also be routinely disposed of.

Retention periods for email messages vary according to the functions they are associated with. It is the responsibility of the agency to codify retention practices through development of records schedules in cooperation with the Kentucky Department for Libraries and Archives. Retention requirements cannot be met through routine agency backups, and agency staff must be made fully aware of this and the appropriate schedules that must be created and adhered to.

EAS Appendix G, Guidelines for Managing E-Mail in Kentucky State Government, promulgated by the Department for Libraries and Archives, provides agencies with further guidance on the implementation of this standard.

Approved Product(s):

Enterprise Standard 2600 establishes Microsoft Exchange as the messaging standard for state government.

Justification:

NA

Technical and Implementation Considerations:

In the Exchange/Outlook shared messaging services environment administered by the Governor's Office for Technology on behalf of state agencies (described at http://got.state.ky.us/CSOneService.asp?SERVICE=8), users' email accounts typically include two "stores" of information, (1) mailboxes maintained on GOT servers (Outlook Today folders), and (2) personal folders stored on agency network servers or users' workstations (in .pst folders). Additionally, a third category in the form of "archived" folders may be present.

The normal size of GOT-maintained mailboxes is limited for reasons of cost to twenty-five megabytes. Backup of mailboxes occurs nightly, with backup tapes being retained for ten days. At any time, if users delete items from their deleted items folders, those items are no longer retrievable unless they were previously captured on backup tapes.

For personal folders, rules relating to the size, number, location of folders (workstation or network server), and backup frequency are established by individual agencies. In instances where agencies permit personal folders on user workstations, no backup may be occurring at all.

Efforts to enhance management of agency email resources must encompass email records

in any of these three forms/locations. Meeting records management and open records requirements solely through reliance on backups of email stores is not a viable option.

Emerging Trends and Architectural Directions:

The sheer volume of electronic mail, its role in the conduct of business, and especially the increasing frequency with which it is being sought and used in court cases, by the press, and by individuals, all are putting increased pressure on public and private sector entities to manage email more effectively. Larger organizations are increasingly acquiring software to facilitate auto-classification of email, content management, or compliance archiving, but state governments, probably for reasons of cost, are only beginning to explore such tools. Microsoft's growing reliance on XML and on forthcoming products like InfoPath offer state government the promise of better tools, but at this time, continued monitoring of best practice is the primary strategy.

Review Cycle:

Annually

Timeline:

Revision date: May 9, 2003
Effective date: March 8, 2001

Enterprise Standards:
5000 Security Domain

Category:
5515 Secure Transport

Definition:
Several network services are available that offer transport security. Secure Sockets Layer (SSL) is a protocol for transmitting private data via the Internet. SSL works by using a private key to encrypt data that is transported over the SSL connection. SSL establishes a secure communications channel between the server and the client web browser. Web browsers such as Netscape Navigator and Internet Explorer support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers and other personally identifying information. A virtual private network (VPN) is a private network configured within a public network infrastructure. A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. On the server side, digital certificates act as electronic credentials to authenticate sites to customers and to enable secure, encrypted transactions and communications using the SSL protocol.

Rationale:
Many electronic government services and electronic commerce transactions are conducted via the Internet, and specifically the web. When the privacy and security of these transactions is paramount, a secure transmission is critical. With electronic commerce transactions, three components are required for secure online commerce: authentication, message privacy and message integrity. With digital certificates issued to secure the server, users know the server is owned and operated by a legitimate organization, such as state government. Since SSL encrypts all traffic between the web server and customers, the content is secure and private - the information cannot be viewed if it is intercepted by unauthorized parties. With message integrity, both parties involved in the transaction know that the content has not been altered and they are seeing exactly what the other party sent.

Approved Standard(s):
Secure Socket Layer (SSL) 3.0 encryption (minimum 40-bit) is required if data needs to be secured via the Internet.

All electronic payments (credit card, EFT, etc) and the collection of personally identifiable information must be secured during transport (see Category 3505 Network Services - Electronic Commerce and Payments). Strong encryption (128-bit) is recommended and may be required for certain applications, particularly personal and health-related information as prescribed in federal law.

To authenticate and secure the web server, a server certificate (digital ID), available from Entrust, must assigned to the web server. This includes secure servers operated under contract, although any server certificate software may be used in those instances. See Category 3510 Network Services - Internet/Intranet Web Server.

Approved Product(s):
Entrust.net Secure Socket Layer (SSL) server certificates
Both web browser approved products (Category 3511) support SSL 3.0
Both web server approved products (Category 3510) support SSL 3.0

Justification:
Secure Socket Layer (SSL) is the recognized and accepted protocol for securing transport on the Internet. Entrust provides a secure and scalable solution and the certificates that are automatically trusted by browsers. These certificates have 128 bit support, multi-year certificates, automatic certificate revocation checking, support for lifecycle monitoring and certificate revocation service and guaranteed notification of web server certificates expiration.

Technical and Implementation Considerations:

Transport security should match the business need of the agency. Strong encryption (128-bit) may be required for certain applications or instances where highly confidential information such as banking, finance and health data is transmitted.

State government has limited experience with internet-based virtual private networks (VPN) that provide secure communications through a combination of tunneling, encryption, and user authentication. Tunneling links two network devices such that the devices appear to exist on a common, private backbone. Encryption and user authentication provide necessary security services for private traffic being transported on the public network, such as the WAN. Since a VPN physically shares the public network, it uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Regarding client software, the approved browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured server the browsers will by default, show an alert warning in a pop-up box. In contrast, if a user submits credit card or other information to a site with a valid server certificate and an SSL connection, the warning does not appear. Another protocol for transmitting data securely over the web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a browser client and server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing transport security technologies. Both protocols have been submitted to the Internet Engineering Task Force (IETF) for approval as standards.

Emerging Trends and Architectural Directions:

Review Cycle:

6 months

Timeline:

Revision date: February 1, 2001
Effective date: June 1, 1999

Appendix D

Response From the Finance and Administration Cabinet*

Recommendation 3.1

The acceptable use task force should consider making the following additions or improvements to the Internet and e-mail acceptable use policy (AUP) and all related policies:

Early this year, Secretary Robbie Rudolph assembled a team to research and write the Internet and E-mail Acceptable Use Policy. Secretary Rudolph invited all identifiable stakeholders to participate, including the Personnel Cabinet, Legal and the Commonwealth Office of Technology. This was done to ensure that the policy would be supported to and adhered to by all state executive agencies. Currently, this policy is in the transition process from policy to administrative regulation. Since the task force feels that it has completed its assignment, it has disbanded. However, when additional issues arise that need to be addressed by all stakeholders, the meetings might once again resume. Although the task force does not meet on a regular basis, policy makers have and will continue to consider and evaluate the recommendations brought to our attention by the LRC study.

- **Describe the range of disciplinary consequences;**

We feel that this question might be more appropriately addressed by the Personnel Cabinet.

- **Describe or reference the basic investigational process and state whether the results will be kept confidential;**

The draft Forensics Policy addresses the issue of investigatory procedures and confidentiality. We will consider the possibility of including it in the Acceptable Use Policy.

- **Explicitly prohibit downloading e-mail from personal e-mail services;**

We feel the policy supports the incidental use of personal e-mail. The purpose of the acquisition of the CSM solution was to mitigate all security concerns associated with the use of commercial e-mail services. All web-enabled e-mail services are inspected by the CSM solution for hostile code and virus infections. By not allowing employees to use personal e-mail systems we will create opportunities for the misuse of the state's e-mail system and create an environment that's not "employee friendly".

- **Describe all aspects of handling confidential information, including secure storage and secure transmission;**

COT has adopted the Entrust product suite for secure communications, which includes e-mail and data encryption.

* The quotes from recommendations are from an earlier draft of this report. Some recommendations have been revised for clarity for this published report.

- **Define procedures to secure private information contained in system logs;**
  Log file access is restricted to network administrators. Access privileges require a valid username and complex password. COT will evaluate current procedures on handling system logs to determine whether any changes should be considered.

- **Require employees to follow all computer safety and security practices;**
  This is a behavioral issue that must be addressed by management within each agency. COT has created and distributed enterprise policies related to computer security and safety. Additionally, COT distributes a security awareness newsletter on a bi-monthly basis that communicates information regarding enterprise security policies. The newsletters also contain security articles, best practices, tips and other ideas on how to be more secure.

- **Mention that the Commonwealth has the right to recover any costs of inappropriate employee computer use;**
  Under the authority of the CIO, COT has the ability to recover any costs associated with computer misuse. Traditionally, these costs have been related to extraneous personnel costs associated with resolving computer virus.

- **Require all employees to receive training on the AUP and related policies, including a thorough explanation of the need for the policies and procedures;**
  The Personnel Cabinet should address this issue.

- **Specify a minimum retention period for system logs, even if the logs are to be discarded daily, and require all agencies who create such logs to adopt their own specific standard;**
  COT agrees that the retention of logs is necessary when relevant to security. Log retention enables adequate review and event correlation. On the other hand, all systems logs aren't required for this purpose and the storage of such logs would impose significant costs for the Commonwealth. COT feels that system logs should be utilized as a real-time management tool for performance and audit review and should be retained for no longer than 10 – 15 business days. The review process will vary depending on the agency size, the number of information systems they support and qualified technical staff available to conduct the reviews.

- **Change the phrase "executive cabinets" to include all executive agencies;**
  We have no issue with this recommendation.

- **Direct all agencies to specify a minimum retention period for personal and transient e-mail records.**
  COT suggests the policy allow incidental use of personal e-mail services for state employees.

Recommendation 3.2

The acceptable use task force should review the applicability of acceptable use policies to all possible users of executive branch computer resources. If any type of user appears not to be covered, the task force should take steps to ensure that the policies can be applied.

The Finance and Administration Cabinet will review the possibility of business agreements that define acceptable use of cabinet services. These services will include technology resources for all agencies outside of the executive branch.

Recommendation 3.3

The Personnel Cabinet and the personnel staff of each agency should implement an ongoing process to establish and promote a corporate culture of proper use of Commonwealth computer resources. The agencies should consider including:

- **Prevention of inappropriate use, beginning with the hiring process and including post-hiring strategies;**
- **Developing an employee education program that explains the reasons for and benefits of acceptable computer use;**
- **Training supervisors to notice personal problems that might lead to inappropriate use and to take corrective action;**
- **Involving employees in the development of acceptable use policies and procedures;**
- **Having procedures for employees to provide feedback and to report violations;**
- **Training supervisors to build a culture that creates loyalty, dedication, and motivation;**
- **Ensuring that policies and procedures are implemented and enforced uniformly within administrative units;**
- **Giving regular feedback to employees on the level and cost of misuse in their department or division over time;**
- **Giving regular feedback to employees on their own computer system use patterns;**
- **Requiring employees to receive ongoing training on their role in computer system security;**
- **Ensuring that every employee has access to a responsive computer assistance and problem reporting process;**
- **Considering adoption of an "open office" or "visible monitor" policy; and**
- **Considering elimination of web access on workstations that do not require it.**

Recommendation 3.4

The Personnel Cabinet should assure that the Kentucky Employee Handbook section related to use of information technology resources is always as accurate and comprehensible to employees as possible.

Recommendation 3.5

The Commonwealth Office of Technology and the information technology office of each agency should consider taking the following actions to manage file storage, local network capacity, and workstation security:

- **Implement storage resource management or similar tools to limit the types and sizes of files that can be transmitted on the local network and stored on file servers and (to the extent possible) on workstations;**

COT currently provides file size and type limitations for e-mail users. We will review the options and toolsets available to limit or prohibit the type and size of files that can be stored on the network infrastructure, including servers and workstations. Implementation options will be considered based on applicability, feasibility and cost.

- **Use file access controls to restrict users to files and storage locations that are appropriate for their work;**

COT agrees with the recommendation and encourages agency administrators to protect information by following the best practices procedures and guidelines. Various sources of information are available for best practices relating to file and share permissions.

- **Use file access controls, encryption, and other techniques to protect confidential or sensitive information;**

The enterprise IT standards have adopted the Entrust product suite for providing secure communications. The Entrust PKI services include e-mail encryption, file storage encryption and digital signature, which may be used together to protect confidential or sensitive information.

- **Maintain up-to-date and patched operating software and antivirus software on all workstations and servers;**

COT has created policies and best practices for server and workstation management. Currently, COT is reviewing an enterprise approach for supporting all Commonwealth workstations with toolsets that can provide a more centralized approach. Acceptance of options will be considered based on applicability, feasibility and cost.

- **Set all workstations to lock up if unused after 10 to 15 minutes and to require a password to reactivate; and**

An enterprise policy for securing workstations already exists and has been implemented by the Finance and Administration Cabinet. The Finance and Administration Cabinet has strongly encouraged other state agencies to adopt this policy.

- **Limit workstation user permissions so that users cannot install any software or hardware and cannot change any sensitive system settings.**

COT agrees with this recommendation on first glance, however, we will conduct a more thorough investigation and will perform an impact analysis.

Recommendation 3.6

The Finance and Administration Cabinet should consider allowing access to non-work-related Internet sites that are appropriate for personal use, consistent with the overall philosophy of CIO-060. If such use is allowed, it should be in the context of good supervisory practice at the agency level.

COT feels the current acceptable usage policy allows for incidental use. It is in the director's discretion as to what is acceptable use for their agency.

Recommendation 3.7

The Personnel Cabinet should design outcome measures to determine the effectiveness of acceptable use management on employee knowledge and behavior, including employee knowledge and support of the policies and inappropriate use incidents and their disposition. All agencies should be required to apply these measures at least annually and to report the results to the Personnel Cabinet. The Personnel Cabinet should compile the results and make them available for review.

Recommendation 3.8

In addition to bandwidth use, the Commonwealth Office of Technology should retain adequate information about web access and e-mail use to track important factors over time. This information should be archived for several years for comparison. COT should consider providing breakdowns by such categories as day of week, period of time (work hours, evenings, weekend days), and web site category, as well as by agency (at the department or division level or lower).

COT's approach to manage Internet and e-mail is based on performance and capacity management. Our practice has been to focus on the enterprise, not specific agencies and their departments. However, we will review this recommendation to see if there are any additional benefits that could be obtained.

Recommendation 3.9

The Commonwealth Office of Technology should:

- **Increase the frequency of required vulnerability testing for agencies and expand its scope to include all systems, not just critical systems. Specifications should include tests of employee alertness and responsiveness to cyber attacks and especially to social engineering espionage.**

COT's original recommendation was that all critical business systems are required to have annual vulnerability tests performed. Due to the adverse budgetary impact to the agencies, the policy was amended to once every two years. This task would be much

easier to perform if the Executive branch agencies had a common data center and adopted server virtualization. This would reduce the number of servers that would have to be evaluated and minimize costs.

- **Conduct periodic tests of the content security management system. These tests should determine whether a user can bypass the rules to gain access to prohibited web sites or to send or receive prohibited types of e-mail.**

The CSM Product has been setup with an automated process to provide the vendor with information that will assist them in providing daily updates to the systems. These updates will enhance the rule base and CSM's ability to protect the Commonwealth. COT will also conduct regular reviews of data that will be reported to the appropriate staff. Several areas will be reviewed to include CSM performance on web site blocking of inappropriate sites, Spam Blocking and Peer-to-Peer related issues.

- **Conduct periodic stress tests of the content security management system, as well as other protective systems, to ensure that they work properly under high-traffic conditions, such as when capacity has been exceeded.**

Periodic performance reviews of the CSM systems will evaluate the overall systems ability to process a vast number of items. Areas such as Disk Usage, Memory and Processor stress levels will be measured on a periodic basis.

Recommendation 3.10

The Personnel Cabinet and the Finance and Administration Cabinet should review acceptable use policies and procedures at least annually. The review should ensure that they work properly, that they comply with the law, and that they use technology effectively. The review could be undertaken through a task force that includes representatives from these cabinets. A Permanent High-level, Multi-agency Team Is Needed

Enterprise policies are reviewed on an annual basis by the Commonwealth Technology Council (CTC). The CTC is comprised of agency Information Technology Officers (ITOs) from all the major state agencies, including the Personnel Cabinet.

Recommendation 3.11

The Personnel Cabinet, Finance and Administration Cabinet, and Governor's Office should formalize the acceptable use task force as a permanent entity with responsibility to review all policies and procedures related to acceptable computer use on a regular basis, oversee their management, and communicate their status to the Governor and to executives in all agencies.

The Commonwealth Technology Council (CTC) has a formal process in place for the adoption of new enterprise policies. The process also includes the responsibility to review and update all policies on a regular basis.

Appendix E

Response From the Personnel Cabinet

In follow up to your request to the Personnel Cabinet, we have completed our review of your draft report dated September 7, 2004. Please note we have concentrated our review to the specific recommendations directed to the Personnel Cabinet and not all of state government. We understand the Finance and Administration Cabinet will be responding as to the implications to their agency. We address only your recommendations as follows:

Recommendation 3.3: We believe this recommendation must also include the Commonwealth's Office of Technology (COT) as statutorily they are charged with implementing and promoting the proper use of the state's computer resources. Specifically, Kentucky Revised Statutes 42.029(e) prescribes the Division of Support Services shall be responsible for training. Also, paragraph 8 of this same statute grants broad authority for the promulgation of "necessary administrative regulations for the furtherance of this section." For these reasons, the inclusion of COT is vital to the success of this recommendation.

Recommendation 3.7: This recommendation must include COT as well as they are the entity with the technical expertise, statutory authority, and personnel to compile and store data regarding use of the state's computer resources. In support, KRS 42.029(b) prescribes, "The Division of Computer Services…shall be responsible for all computer operations…data storage." The Personnel Cabinet does not have the personnel, expertise, technical systems or statutory authority to carry out this recommendation.

Further, the Personnel Cabinet would need additional personnel, expertise and hardware to carry forward a number of the recommendations mentioned in the report. Additional funding would also be required for many services and positions already existing within the Commonwealth's Office of Technology. Finally, we suggest Recommendation 3.11 be moved to the top of the list as the creation of the task force and their mission is integral to the majority of the recommendations delineated throughout the report.

Please feel free to contact us if we may be of further assistance.

Sincerely,

Howard "Burr" Lawson
Executive Director
Office of Administrative Services