SpectorSoft®

White Paper

Bringing Your Internet Acceptable Use Policy Up to 2010 Standards

SpectorSoft Corporation
1555 Indian River Blvd.
Vero Beach, FL 32960

1.888.598.2788 toll-free
1.772.770.5670 sales and support

www.spector360.com

Table of Contents

Introduction 3

The Business Impact of Internet Abuse 3

What is an Internet Acceptable Use Policy? 4

Why Should I Implement an IAUP at My Company? 5

Financial and Technological Reasons for Implementing an IAUP 5

Using an IAUP to Protect Sensitive and Confidential Company Information 5

Informing and Educating Users 6

Developing an Internet Acceptable Use Policy 6

Example Internet Acceptable Use Policy 7

SAMPLE INTERNET ACCEPTABLE USE POLICY

ELECTRONIC ACCESS POLICY

I. General 9

EMAIL

II. Email Policies and Procedures 9

NETWORK AND INTERNET POLICY

III. Personal Responsibility 11

IV. Permitted Use and Terms 11

V. Availability and Access 11

VI. Content and Communications 11

VII. Privacy 11

VIII. Downloaded Files 12

IX. Confidential Information 12

X. Prohibited Activities 13

XI. Computer Equipment 14

XII. Compliance 14

XIII. Noncompliance 14

SOFTWARE USAGE POLICY

XIV. Software Usage Policies and Procedures 15

XV. Electronic Access Policy 16

About Spector 360®

Spector 360 enables you to monitor employee PC and Internet use, analyze trends and patterns, search for specific details, investigate when something seems amiss, and report your findings all from the convenience of your desktop. Spector 360 is a highly scalable, centrally-managed, employee monitoring solution that is easy to deploy and manage, even company-wide.

Features at a Glance

- Monitor all employee PC and Internet activity with high-level charts, graphs and tables
- View detailed activity of individual employees with point-and-click drill down
- Automated reporting
- Includes context-based web filtering
- Multiple levels of security prevent tampering or disabling
- Configure, install and manage over existing network

PC MAGAZINE EDITORS' CHOICE
September 2008
Spector 360

"Top-notch reporting and monitoring"

"Highly configurable and scalable"

"Well-designed client server architecture"

-PC Magazine

Introduction

Organizations of all sizes rely on the Internet as an essential tool to conduct business and communicate with employees, customers, partners and external audiences. Most organizations encourage their employees to use the Internet to conduct business as well as for personal use within "acceptable limits," despite the fact that Internet abuse costs businesses millions of dollars in lost productivity each year. Establishing acceptable use limits and clearly communicating these to employees can help minimize Internet abuse, lost productivity, leaking of confidential information, and other inappropriate activities that can expose a business to financial, legal, compliance, and other preventable risks.

The Business Impact of Internet Abuse

Misuse of the Internet at work started to gain media attention in the early 1990s primarily as a concern over wasted time. Since then, it has escalated into a multi-billion dollar problem for businesses each year. In addition to tangible dollar losses due to lack of productivity, very serious and costly threats can occur when employees act or click on something they shouldn't from a work computer.

Human behavior studies have shown that people act differently when they're in front of a camera, versus when they think nobody is watching. This is one of the reasons why PC and Internet monitoring software, such as Spector 360 (www.spector360.com), is rapidly becoming a "must have" in the business world. It fills a gap in traditional wall-and-fortress security approaches by monitoring the human element of IT security and exposing active threats from:

- **Productivity Losses:** The average employee wastes more than 81 minutes of work time per day doing non-work-related surfing, which in turn costs US employers an estimated $750 billion in lost productivity each year. [Business Week]
- **Data Theft:** As many of 41% of employees admit to taking sensitive company data with them to a new job, and 26% will pass it on to help friends or family land a job. [eChannelLine USA]

Learn more about SpectorSoft monitoring and surveillance solutions for business at **spectorsoft.com**

SpectorSoft®

SpectorSoft Corporation
1555 Indian River Blvd.
Vero Beach, FL 32960

888.598.2788 toll-free
772.770.5670 sales and support

www.spectorsoft.com

- **Online Pornography:** 70% of all web traffic to Internet pornography sites occurs during the work hours of 9:00 a.m. to 5:00 p.m. [Business Week]

- **Socially Engineered Attacks:** The number of companies reporting spyware and malware attacks via social networks in 2009 increased by 70%. [Sophos]

- **Business Networking:** LinkedIn has more than 50 million members; Twitter has 75 million accounts and generates approximately 1.3 million Tweets per hour. More than 700,000 businesses have active pages on Facebook. [eConsultancy]

- **Social Networking:** Facebook boasts 350 million users, half of which are on the site every day. More than 3.5 billion pieces of content are shared each week on Facebook. [Facebook]

- **Personal Email and Webmail:** 82% of employees use their personal email accounts to send large work-related files. [Osterman Research]

- **Compliance Violations:** High-profile HIPAA violations became increasingly prevalent last year. Fines can be substantial – up to $250,000 – and criminal penalties can also be imposed. Violations can also impart significant reputation and brand damage. [ZDNet]

Given the tangible impact and losses that can stem from a single incident in any one of the above areas – or several occurring simultaneously across an entire organization – it is clear that productivity, ethics, security and compliance concerns must be addressed head on by regulating employee Internet use. Establishing guidelines for acceptable use of the Internet and computing resources requires planning, management, enforcement, and a well-defined and communicated policy as a foundation.

What is an Internet Acceptable Use Policy?

An Internet Acceptable Use Policy (IAUP), also known as an Acceptable Use Policy or Use Policy, is a written, legally binding agreement that is signed by employees with the intent of identifying the permissible workplace uses of the Internet. It also serves to let employees know that all activity on company-supplied computers, laptops, PCs and Macs may be monitored in accordance with the law.

An IAUP should specifically set out prohibited uses, rules of online behavior, and access privileges. Penalties for violations of the policy, including security violations and vandalism of the system, should also be covered. Anyone using a company's Internet connection should be required to sign an IAUP, which will be kept on file and may be subject to future revision as company policies and technology changes. Communicating these guidelines ensures that employees are fully informed of company policies and expectations, and lets the business address productivity, ethics, security, and compliance concerns head on.

With rapid advancements that took place in 2009 with Internet-based programs and social media sites like Facebook, Twitter and LinkedIn, this may be a good time to either implement an IAUP or to bring your existing policy up to 2010 standards.

Why Should I Implement an IAUP at My Company?

The Internet can be a magnificent source of detailed, current information that can enhance employee productivity and business success. The Internet also allows access to a vast amount of purely entertainment-related features. Providing access to the Internet carries the same potential for productivity drain as placing a television on every employee's desk.

It is not surprising then, that loss of productivity is the number one reason for drafting an IAUP. Another reason to institute an IAUP is to shield an employer from possible sexual harassment suits. Many Internet sites offer unrestricted access to pictures, video, sound, and text that is sexually oriented. If such material is brought into the workplace, it carries with it the potential to create a hostile work environment, thereby presenting a potential risk of exposure to the employer under federal or state prohibitions against sex discrimination.

Financial and Technological Reasons for Implementing an IAUP

Restricting use of the Internet to only work-related matters serves to prevent a drain on limited computer resources caused by frivolous use. Access to the Internet costs businesses money, either in fees to Internet Service Providers, or in hardware costs necessary to accommodate increased network traffic and data storage.

An employee's inappropriate use may negatively affect other employees' speed of access or storage space for work product. An IAUP can guide employees concerning the use of storage space and bandwidth on the system to maximize utility to all employees. Examples of restrictions serving this interest would be directives against downloading games or other non-work related files, restrictions on downloading large files that can be obtained off-line, and instructions to move old or seldom used files, programs or email to alternative storage.

Using an IAUP to Protect Sensitive and Confidential Company Information

Employers who have sensitive data on their computer system such as company plans, customer demographic data, or product designs may need a clause in their IAUP concerning trade secrets. It should be made clear to employees that under no circumstances should proprietary company information be transmitted via personal email or Web-based email, file-sharing sites, instant messages, social networking sites, or passed though the Internet or that such material be encrypted if transmitted over the Internet within acceptable guidelines.

Employers should institute guidelines that prohibit illegal use of the Internet in general. A directive that employees take care not to violate copyright laws should be included in every IAUP. Gambling via the Internet may also be a concern with the rise in online gambling sites and even Fantasy Football leagues. An IAUP should contain a prohibition against such activity not only because of its potentially adverse affect on productivity but also because in many cases, online gambling activity may be illegal.

Informing and Educating Users

Changing company culture and habits takes time and effort, especially when new policies are introduced. As a complement to your IAUP, consider creating a short training program and administering it to new employees and contractors before they are allowed to have Internet privileges. This serves to educate them on properly accessing email servers and browsers, and what will not be tolerated from a legal, ethical and security standpoint. Introductory training programs can set new expectations and break old habits that people bring with them. Ongoing training programs, such as company-wide email reminders, newsletter articles, or Intranet-based polls and quizzes, can remind employees about certain aspects of a company's policy or educate them when new threats, viruses and socially engineered attacks become a concern.

Developing an Internet Acceptable Use Policy

The goal of an Acceptable Use Policy is to translate, clarify and communicate management's position on acceptable uses of Internet access and company-provided IT resources, including but not limited to computer systems, laptops, servers, and even printers. The policies defined in an IAUP act as a bridge between management objectives and specific employee requirements. Therefore, a good IAUP must:

- Be **clear** and **implementable** by employees. Using terms like "reasonable" and "not appropriate" are subject to interpretation and should be avoided. Setting clear expectations like: "employees are permitted personal use of the Internet during their lunch hour and for no longer than a total of 15 minutes throughout the work day," can easily be understood and more effectively regulated.

- Be **enforceable** by the IT staff and management. This may require an investment in third-party monitoring, filtering and security solutions to allow the company to investigate and confirm when violations occur.

- Clearly define the areas of **responsibility** for employees, administrators and management.

- Be **documented**, **distributed** and **communicated** to all parties governed by it.

- Be **flexible** to stay in lockstep with changes in IT infrastructure, security threats, and employee use of Internet resources for work and non-work. Plan to revisit the IAUP regularly to ensure that policies do not become obsolete; or at a minimum, once a year.

Before mapping out an IAUP, employers should perform a baseline assessment of employee Internet and PC usage for several weeks. This will allow an employer to understand the scope of activity within the company, and craft a more effective IAUP for those who will be governed by it.

Example Internet Acceptable Use Policy

On the following pages is a sample Internet Acceptable Use Policy for reference purposes only. If you use any of this language in your own IAUP, you might want to have a lawyer review it for viability.

SpectorSoft®

Sample

Internet Acceptable Use Policy

SpectorSoft Corporation
1555 Indian River Blvd.
Vero Beach, FL 32960

1.888.598.2788 toll-free
1.772.770.5670 sales and support

www.spector360.com

ELECTRONIC ACCESS POLICY

I. GENERAL

The Company provides some, if not all, employees with electronic access, consisting of an email system, a network connection, and Internet/Intranet access. This policy governs all use of the Company's network, Internet/ Intranet access, and email systems at all Company locations and offices. This policy includes, but is not limited to, electronic mail, chat rooms, the Internet, news groups, electronic bulletin boards, the Company's Intranet and all other Company electronic messaging systems.

EMAIL

II. EMAIL POLICIES AND PROCEDURES

The Company's email system is designed to improve service to our customers, enhance internal communications, and reduce paperwork. Employees using the Company's email system must adhere to the following policies and procedures:

- The Company's email system, network, and Internet/Intranet access are intended for business-use only. Employees may access email and the Internet for personal use only during non-working hours, and strictly in compliance with the terms of this policy.
- *All information created, sent, or received via the Company's email system, network, Internet, or Intranet, including all email messages and electronic files, is the property of the Company. Employees should have no expectation of privacy regarding this information. The Company reserves the right to access, read, review, monitor, copy all messages and files on its computer system at any time and without notice. When deemed necessary, the Company reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.

  *Initials: ___________
- Use extreme caution to ensure that the correct email address is used for the intended recipient(s).
- Any message or file sent via email must have the employee's name attached.
- Personal email accounts are not permitted unless expressly authorized in advance by the Company's Chief Information Officer. Employees are also prohibited from using personal email accounts and Web-based email such as Yahoo Mail, Google Gmail and others, to transmit business information or documents of any kind. All business email should be sent and received via company-provided email.

- Alternate Internet Service Provider connections to the Company's internal network are not permitted unless expressly authorized by the Company and properly protected by a firewall or other appropriate security device(s) and/or software.

- Confidential information should not be sent via email unless encrypted by Company approved encryption software and according to established Company procedure in effect at the time of transmittal. This includes the transmission of customer financial information, Social Security numbers, employee health records, or other confidential material.

- Employees must provide the System Administrator and/or Chief Information Officer with all passwords.

- Only authorized management personnel are permitted to access another person's email without consent.

- Employees should exercise sound judgment when distributing messages or posting content on third-party sites like LinkedIn, Twitter, Facebook, MySpace, Flickr, and more. Client-related messages should be carefully guarded and protected. Personal content that is not appropriate for colleagues, employers, customers or partners to view should not be made public to them. The Company asks that you take advantage of privacy settings within Facebook and other sites to ensure that personal comments, images and information remain out of view of business-related contacts whenever appropriate to do so. Employees must also abide by copyright laws, ethics rules, and other applicable laws.

- Email messages must contain professional and appropriate language at all times. Employees are prohibited from sending abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages via email. Sending abusive, harassing, intimidating, threatening, discriminatory, sexual, or otherwise offensive messages via email will result in disciplinary action up to and including termination.

- Email usage must conform to the Company's harassment and discrimination policies.

- Use of the Company's email system to solicit for any purpose, personal or otherwise, without the consent of the Company is strictly prohibited.

- Chain messages and executable graphics and/or programs should be deleted. Any employee engaging in the transmission of inappropriate emails, as determined by management, will be subject to disciplinary action, up to and including termination.

- Employees should archive messages to prevent them from being automatically deleted. All messages archived in the Company's computer system shall be deemed Company property, as is all information on the Company's systems. Employees are responsible for knowing the Company's email retention policies.

- Misuse and/or abuse of electronic access, including but not limited to, personal use during working hours, copying or downloading copyrighted or confidential materials, visiting pornographic sites or sending abusive email messages will result in disciplinary action, up to and including termination.

*** Violation of any of these policies will subject an employee to disciplinary action, up to and including termination.**

NETWORK AND INTERNET POLICY

III. PERSONAL RESPONSIBILITY

By accepting an account password, related information, and accessing the Company's Network or Internet system, an employee agrees to adhere to the Company policies regarding their use. You also agree to report any misuse or policy violation(s) to your supervisor or the Company's Chief Information Officer.

IV. PERMITTED USE AND TERM

Use of the Network and the Internet is a privilege, not a right. Use of Network and Internet access extends throughout an employee's term of employment, providing the employee does not violate the Company's policies regarding Network, Internet or Intranet use.

V. AVAILABILITY AND ACCESS

The Company reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns.

VI. CONTENT AND COMMUNICATIONS

The Company, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be permitted or prohibited.

VII. PRIVACY

* Network and Internet access is provided as a tool for our organization's business. The Company reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the Company. An employee should have no expectation of privacy regarding them. Network administrators may review files and

intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this Policy.

*Initials: __________

VIII. DOWNLOADED FILES

Files are not to be downloaded from the Internet without the prior authorization of management. Any files authorized for download from the Internet must be scanned with virus detection software before being opened. Employees are reminded that information obtained from the Internet is not always reliable and should be verified for accuracy before use.

IX. CONFIDENTIAL INFORMATION

Employees may have access to confidential information about the Company, other employees and clients. With the approval of management, employees may use email to communicate confidential information internally to those with a need to know. Such email must be marked "Confidential." For purposes of this policy, confidential information includes, but is not limited to:

(a) Procedures for computer access and passwords of the Company's clients and customers, program manuals, user manuals, or other documentation, run books, screen, file, or database layouts, systems flowcharts, and all documentation normally related to the design or implementation of any computer programs developed by the Company relating to computer programs or systems installed either for customers or for internal use;

(b) Lists of present clients and customers and the names of individuals at each client or customer location with whom the Company deals, the type of equipment or computer software they purchase or use, and information relating to those clients and customers which has been given to the Company by them or developed by the Company, relating to computer programs or systems installed;

(c) Lists of or information about personnel seeking employment with or who are employed by the Company;

(d) Prospect lists for actual or potential clients and customers of the Company and contact persons at such actual or potential clients and customers;

(e) Any other information relating to the Company's research, development, inventions, purchasing, engineering, marketing, merchandising, and selling.

X. PROHIBITED ACTIVITIES

Employees are prohibited from using the Company's email system, network, or Internet/Intranet access for the following activities:

- Downloading software without the prior written approval of the Company's Chief Information Officer.
- Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.
- Using software that is not licensed by the manufacturer or approved by the Company.
- Sending, printing, or otherwise disseminating the Company's proprietary data, or any other information deemed confidential by the Company, to unauthorized persons.
- Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.
- Searching for outside employment.
- Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. An employee should notify their supervisor and/or Human Resource manager immediately upon receiving such a message. This type of message should not be forwarded.
- Sending or forwarding a message that discloses personal information without Company authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about clients or fellow employees without authorization.
- Sending ethnic, sexual-preference or gender-related slurs and/or jokes via email. "Jokes", which often contain objectionable material, are easily misconstrued when communicated electronically.
- Sending or soliciting sexually oriented messages or images.
- Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, or drugs.
- Gambling or engaging in any other criminal activity in violation of local, state, or federal law.
- Spending excessive time using personal email accounts and social networking sites during company time, for non-business purposes.
- Engaging in unethical activities or content.

- Participating in activities, including the preparation or dissemination of content, which could damage the Company's professional image, reputation and/or financial stability.
- Permitting or granting use of an email or system account to another employee or persons outside the Company. Permitting another person to use an account or password to access the Network or the Internet, including, but not limited to, someone whose access has been denied or terminated, is a violation of this policy.
- Using another employee's password or impersonating another person while communicating or accessing the Network or Internet.
- Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the Company's computer systems.

XI. COMPUTER EQUIPMENT

The following policies are designed to reduce repair costs, maintain the integrity of our system and protect the Company's assets. Employees should adhere to the following:

- Do not keep liquids or magnets on or near the computer.
- Do not remove any computer from the building without written permission from management.
- Do not transport recordable media back and forth between home and office, including recordable CDs and DVDs, thumb drives, portable hard drives, and personal laptops. If company-related presentations, documents and email need to be accessed on iPhones, BlackBerries, smartphones, Netbooks and other devices, please be sure to password protect them. This will help minimize exposure to viruses or prevent data loss if such devices are stolen.

XII. COMPLIANCE

Though each individual is responsible for his/her own actions, management personnel are responsible for ensuring employee compliance with Company policy.

Any employee aware of a policy violation should immediately report the violation to their supervisor, the Company's Chief Information Officer and/or the Human Resource manager.

Employees who violate this policy and/or use the Company's email system, network, Internet, or Intranet access for improper purposes will be subject to disciplinary action, up to and including termination.

XIII. NONCOMPLIANCE

Violation of these policies will result in disciplinary action up to and including termination.

SOFTWARE USAGE POLICY

XIV. SOFTWARE USAGE POLICIES AND PROCEDURES

Software piracy is both a crime and a violation of the Company's Software Usage Policy.

Employees are to use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by designated managerial personnel) is a violation of copyright law. In addition to being in violation of the law, unauthorized duplication of software is contrary to the Company's standards of employee conduct.

To ensure compliance with software license agreements and the Company's Software Usage Policy, employees must adhere to the following:

1. Employees must use software in accordance with the manufacturer's license agreements and the Company's Software Usage Policy. The Company licenses the use of computer software from a variety of outside companies. The Company does not own the copyright to software licensed from other companies. Employees acknowledge they do not own software or its related documentation. Employees may not make additional copies of software, unless expressly authorized by the software publisher. The only exception will be a single copy, as authorized by designated managerial personnel, for backup or archival purposes.

2. The Company does not condone and prohibits the unauthorized duplication of software. Employees illegally reproducing software will be subject to disciplinary action. In addition, employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

   NOTE: Unauthorized reproduction of software is a federal offense under US and Canadian copyright laws. In the United States, violators may be subject to civil damages in amounts up to $150,000 per title copied. Criminal penalties include fines as high as $250,000 per software title copied, and imprisonment of up to 5 years.

3. Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the Company, or who places or uses unauthorized software on the Company's premises or equipment shall be subject to disciplinary action, up to and including termination.

4. Employees are not permitted to install their personal software onto the Company's computer system. Employees are not permitted to copy software from the Company's computer system for installation on home or other computers without prior authorization.

5. In cases that require an employee to use software at home, the Company will purchase an additional copy or license. Any employee issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the Company. Employees who are required to use software at home should consult with the Chief Information Officer or Systems Administrator to determine if appropriate licenses allow for home use.

6. Employees are prohibited from giving software or fonts to clients, customers, vendors, and other persons not in the employ of the Company. Under no circumstances will the Company use software from an unauthorized source, including, but not limited to, the Internet, home, friends and/or colleagues.

7. Employees who suspect or become aware of software misuse are required to notify their supervisor, Chief Information Officer, Human Resources manager, or department manager.

8. All software used on Company-owned computers will be purchased through appropriate procedures. Consult your supervisor, Chief Information Officer, Human Resources manager or department manager for proper procedures.

XV. ELECTRONIC ACCESS POLICY

Acknowledgement of Receipt and Understanding

I hereby certify that I have read and fully understand the contents of the Electronic Access Policy. Furthermore, I have been given the opportunity to discuss any information contained therein or any concerns that I may have. I understand that my employment and continued employment is based in part upon my willingness to abide by and follow the Company's policies, rules, regulations and procedures. I acknowledge that the Company reserves the right to modify or amend its policies at any time, without prior notice. These policies do not create any promises or contractual obligations between this Company and its employees. My signature below certifies my knowledge, acceptance and adherence to the Company's policies, rules, regulations and procedures regarding Electronic Access.

Signature ____ Date ____________

Acknowledged by: ____________________________________ Date ____________