



USAGE OF COMPANY-PROVIDED E-MAIL AND INTERNET ACCESS SERVICES

I. PURPOSE AND SCOPE

To establish a uniform policy for employee usage of e-mail programs utilized by the company and employee usage of company-provided Internet access services. This policy applies to all employees of Federal Signal Corporation and its subsidiaries.

This policy is designed to help Federal Signal Corporation employees understand expectations and guidelines regarding company-provided e-mail and Internet resources.

All existing company policies apply to an employee's conduct on the Internet, including those dealing with intellectual property, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

Connection to the Internet can present significant risks to data and systems if appropriate security discipline is not followed. An Internet user can be held responsible for any breach of security or confidentiality resulting from improper usage.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, reduces productivity, consumes supplies, and unnecessarily engages printers and other shared resources. It may also expose the company to negative publicity and significant legal liabilities.

II. TERMS

Certain terms in this policy should be understood to include related thoughts:

"Company" includes Federal Signal Corporation and its related companies.

"Document" includes any file that can be viewed on a computer screen, including electronic mail text, HTML files read in an Internet browser, any file accessed by a word processing, spreadsheet, or desktop publishing program or its viewer, or the files prepared for other electronic publishing tools, such as Adobe Acrobat reader.

"Graphics" include photographs, pictures, animation, movies, or drawings.

"Display" includes CRT monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

"Download" is the process of copying or moving files from an Internet source to a company computer or network. This includes files attached to electronic mail messages.

"Virus, worms and Trojan Horse" are software programming designed to corrupt computer files. The typical pattern of transmission is as an e-mail attachment.

III. PROVISIONS

A. Privacy

The company reserves the right to utilize software and systems to monitor and record all Internet and e-mail usage. These security systems are capable of recording each World Wide Web site visit, chat, newsgroup or e-mail message, and each file transfer into and out of internal networks. No employee should have any expectation of privacy as to his/her Internet usage. Company managers will review Internet activity and analyze usage patterns. They may choose to use this data to assure that company Internet resources are devoted to maintaining productivity. The company reserves the right to inspect all files stored on its computers, networks, or other storage media to assure policy compliance.

B. Offensive Content

The display of any kind of sexually explicit image or document on any company system is a violation of our sexual harassment policy. In addition, such material may not be archived, stored, distributed, edited or recorded using company resources. The company may use independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites. If you find yourself accidentally connected to a site that contains sexually explicit or offensive material, you must disconnect immediately.

If you receive a sexually explicit or offensive e-mail or e-mail attachment from another employee of Federal Signal Corporation or its subsidiaries, you are required to notify your human resources manager as soon as possible.

C. Software Downloads

Employees with Internet access may only download software for business use, and must arrange for proper licensing and registration. Any such files or software are to be used consistent with their licenses or copyrights.

Any programs that are downloaded to a company computer must be approved by the Information Technologies Department. Software or files downloaded via the Internet become company property.

Files downloaded from the Internet must be scanned for viruses prior to usage. Employees may not use the company's Internet facilities to propagate any virus, worm, Trojan horse, or trap door program code.

D. Lawful Use

Company Internet facilities and computing resources must be used in accordance with the laws and regulations of the United States, and any country in which the company maintains a business presence as well as those of any web hosting nation, state, city, province or other local jurisdiction. Such laws include, but are not limited to, copyright, trademark, liable, slander, and public speech control. Use of any company resources for illegal activity is grounds for immediate dismissal and the company will cooperate with any legitimate law enforcement activity.

E. Proper Representation

Employee's using Company Internet facilities shall identify himself/herself honestly when participating in chats or newsgroups, sending electronic mail, or when setting up accounts on outside computer systems.

Only authorized employees or officials may speak or write on behalf of the company to the media, analysts, public gatherings, and newsgroups or in chat rooms. Employees may participate in newsgroups or chats in the course of business when relevant to their duties, but do so speaking only for themselves. Where an individual participant is identified as an employee or agent of this company, he or she must refrain from any political support, endorsement or appearance of company endorsement for any commercial product or service not offered by company, its subsidiaries or affiliates.

F. Copyright & Trademarks

The company retains the copyright to any material posted to any forum, newsgroup, chat, or World Wide Web page by any employee in the course of his/her duties. Company material posted in such a manner must be accompanied by appropriate claims for copyright as determined by company legal staff. Employees with Internet access may not distribute data or software that is licensed or owned by the company without approval from the proper department manager.

G. Confidentiality

Employees are reminded that chats and newsgroups are public forums where it is wrong to tell confidential company information, customer data, trade secrets, and any other material considered confidential. Employees releasing such confidential information - even if the release is accidental - will be subject to discipline in accordance with existing company policies and procedures.

H. Entertainment Software and Games

Employees with Internet access may not use company Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

I. Security

User IDs and passwords help maintain individual accountability for Internet resource usage. A password or ID for an Internet resource from the Company must be kept confidential and should not be shared.

J. News Services

In the interest of keeping employees well informed, use of news briefing services is acceptable, within limits that may be set by departmental activities.

K. Relevance to Other Policies

Company Internet access facilities used to commit infractions such as misusing company assets or resources, sexual harassment, unauthorized public speaking and stealing of intellectual property are forbidden and will be enforced in line with personnel policies.

L. Purposeful Damage

No employee may use the company's Internet facilities to disable, overload or avoid any computer system or network intended to protect the privacy or security of another user. Any employee who attempts to do so will be subject to immediate dismissal.

M. Personal Use

Provided that all above provisions are met, employees may use company Internet facilities for non-business research or browsing during mealtime, breaks, or outside of work hours. Usage must be within reasonable limits as determined by company management. Any files downloaded for personal use may not be stored on company computers, networks, or electronic storage media.

N. Due Care

Employees who receive electronic mail are exposed to software viruses, worms, and Trojan Horses caused by a sender knowingly or unknowingly transmitting e-mails with damaging file attachments. It is important to understand the risk of opening or executing file attachments that contain file extensions (or suffixes), such as “.VBS” or “.EXE”. Employees should maintain their awareness of the typical patterns displayed by e-mail viruses and not open attachments that could potentially corrupt the company’s computer software.

If you receive a warning from a Federal Signal Corporation technology manager about a virus, you are prohibited from opening/initiating the potentially damaging e-mail attachment and you are to report the receipt of the e-mail in accordance with your business unit technology manager’s instructions.

IV. ACKNOWLEDGMENT

The company from time to time will require employees to sign an acknowledgment of each employee’s understanding and compliance with this policy. This acknowledgment form is provided in Exhibit A.

V. DISTRIBUTION OF POLICY

This policy is to be read and understood by all employees of the company who utilize the company’s computer, e-mail or Internet resources. Information services or technology managers are to take steps to see this policy is distributed to all new employees and to provide periodic reminders of this policy to all employees using these resources.

VI. RECORD RETENTION AND DESTRUCTION

For more information regarding the company’s record retention and destruction policy, refer to SPP 2.1.3.

Employee Acknowledgment

I acknowledge that I have received a written copy of Federal Signal Corporation's policy named **Usage Of Company-Provided E-Mail And Internet Access Services**, SPP 1.2.6.

I understand its terms and agree to abide by them. I realize that the company's security software may record and store for management use the electronic e-mail messages I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file.

I understand that any abuse of this policy could lead to my dismissal from employment or criminal prosecution.

Employee Name

Date