Federal Signal Corporation

Standard Policies and Practices

SPP No.
1.2.6

USAGE OF COMPANY-PROVIDED E-MAIL, INTERNET ACCESS SERVICES, AND INFORMATION TECHNOLOGY RESOURCES

I. PURPOSE AND SCOPE

To establish a uniform policy and guidelines for the usage of Company e-mail, Company-provided internet access, and all other Information Technology ("IT") Resources. This policy applies to Company employees, users and its contractors and includes its domestic and foreign subsidiaries (see User definition below).

Various additional Company policies apply to a User's internet usage, including, but not limited to those dealing with intellectual property, privacy, misuse of Company IT Resources, sexual and other harassment, social media, information and data security, and confidentiality.

Connection to the internet can present significant risks to Company data and systems if a User fails to follow appropriate security discipline. Unnecessary or unauthorized internet usage also causes network and server congestion: it slows other Users, reduces productivity, consumes IT Resources, and unnecessarily engages other shared systems. Personal data and software stored on IT Resources also consumes available Information Technology (IT) Resources and may expose the Company to intellectual property claims. Inappropriate personal data or internet usage may also expose the Company to negative publicity and significant legal liabilities. Every User is responsible for managing Company information, which includes protecting confidential and proprietary information and safeguarding the company's reputation. It is expected that Users will use sound and prudent judgement and act ethically in alignment with Federal Signal's Corporate values when:

1. Managing company information.
2. Using IT Resources, whether or not that use is related to their employment duties.
3. Using social media for Federal Signal business or personal reasons.

The Company permits personal use of Company IT Resources subject to reasonable limits listed in Section III. L. of this document.

The Company does not permit storage of or access to inappropriate materials, including materials containing unlawful or offensive content (as defined herein). Further, the Company requires that Users exercise the precautions prescribed herein and follow reasonable and appropriate security discipline. At no time is a personal USB storage

device allowed to be connected to any Federal Signal owned device, including but not limited to computers, laptops, mobile devices, and tablets without the authorization of IT.

Any User who uses any IT Resource in a manner that knowingly causes or subjects the Company to a data security breach or the loss of Company confidential information, or otherwise knowingly violates this or a related policy, is subject to discipline, up to and including termination of employment.

II. TERMS

The following terms in this policy should be understood to include related concepts:

"Company" includes Federal Signal Corporation and its domestic and foreign subsidiaries and affiliated operations.

"Document" includes any file or website that can be viewed on a computer screen, including e-mails, HTML files read in an internet browser, any file created or 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.

"IT Resource" includes any IT Department equipment or virtual technology, including but not limited to, desktop computers, laptop computers, Company issued mobile devices such as cellular phones, smart phones and tablets (including company issued iPads), external/removable media storage devices such as external hard drives and USB drives, network resources including storage locations ("Home" drives or departmental share drives and or 3rd party shared drives like OneDrive), printers and scanners, SharePoint sites, streaming video, social media, network and VPN (Virtual Private Network) access and email, Company software systems and programs, and Company-provided internet access. IT Department-issued credentials, privileges and access should also be viewed as IT Resources.

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

"Download" is the process of copying or transmitting files or data from an internet source or other computer to the computer or network that is in use (typically a Company computer or network). This includes retrieval of files attached to email messages.

"Malware" is a generic term for software programs designed to damage, disable, or otherwise compromise a computer or network of devices. Common examples include viruses, worms, Trojan horses, root kits, ransomware, and spyware.

"Media" is any physical medium used as a vehicle to transfer or distribute digital data. Examples include USB thumb drives, external hard drives, CD's, DVDs, and MP3 devices.

"Upload" is the process of copying or transmitting files or data from the computer in use (typically a Company computer or network) to another computer or network.

"User" is any individual including but not limited to employees, consultants and vendors who have been granted authorization to access any Company IT Resource.

III. PROVISIONS

A. Privacy

The Company reserves the right to utilize software and systems to monitor and record all user internet and e-mail traffic and to inspect all files stored on the Company's computers, networks, or other storage media to ensure that Company internet resources are devoted to maintaining productivity and in compliance with Company policies. No User should have any expectation of privacy as to their internet, email, chat, or computer usage on Company resources.

B. Offensive Content

The display of any kind of sexually explicit image or document on any IT Resource or Company system is a violation of our Equal Employment Opportunity Policy and is forbidden. In addition, such material may not be accessed, archived, stored, distributed, viewed, edited, or recorded using Company IT Resources. Access to any offensive content is not allowed on Company IT resources. The Company may use independently supplied software and data to identify User access to inappropriate or sexually explicit internet sites. Access will be blocked from within our networks to sites identified as such. If a User accidentally connects to a site that contains sexually explicit or offensive material, they must disconnect immediately.

Users must contact their local HR (Human Resources) manager immediately if they receive a sexually explicit or offensive e-mail, e-mail attachment or chat.

C. File and Software Downloads/ Uploads

Users with internet access may not download or upload files or software for illegal or inappropriate use and must arrange for proper software licensing and registration of any software that is downloaded or uploaded and installed. Any such files or software are to be used consistent with their licenses or copyrights. Any programs downloaded or uploaded to a Company IT resource must be approved by the IT Department. Approval is not required from the IT Department to add third-party apps to Company smart phones and similar devices if the app(s) are legally obtained and otherwise complaint with this and other Company Policies. Any pre-approved software or files downloaded or uploaded to Company IT resources become Company property. The IT Department reserves the right to remove software from Company equipment without notifying the User if said software is deemed to be inappropriate, unauthorized, unlicensed or in violation of this or other Company policy. For this reason, Users are discouraged from utilizing personal files or software on any Company computer, and appropriate caution should be exercised when using applications on Company smart phones and similar devices.

Files downloaded from the internet or other external sources must be scanned for viruses prior to usage. Business unit IT support personnel, or the Company IT Service desk, can help with this process. Users must exercise care and common sense and take appropriate measures to ensure that they do not use the Company's internet system to propagate any virus, worm, Trojan horse, or trap door program code or subject the Company's internet system to such malware.

D. Lawful Use

Company internet facilities and IT 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, any web hosting nation, and any state, city, province, or other local jurisdiction. Such laws include copyright, trademark, liability, slander, and public speech control. Intentional use of any IT Resources for illegal activity is grounds for immediate dismissal, and the Company will cooperate with any legitimate law enforcement investigation into that activity.

E. Proper Representation

Users and contractors must use Company supplied accounts (i.e., Email) when conducting company business. Users using Company internet facilities shall identify themselves honestly when participating in chats or newsgroups, when sending e-mail, or when setting up accounts on outside computer systems (such as social media or public online forums).

Only authorized Users may speak or write on behalf of the Company to the media, analysts, public gatherings, and newsgroups or in chat rooms. An authorized User is one who has received specific prior authorization from an Officer of the Company for this purpose. Authorized Users must refrain from any political support, endorsement, or appearance of Company endorsement for any commercial product or service not offered by the Company, its subsidiaries, or affiliates.

When using Company IT Resources and unless authorized by the Company, Users may participate in newsgroups or chats but may do so speaking only for themselves. If identified as a User of the Company, Users must clearly disclose that the views expressed are their own and not that of the Company using the following disclaimer: "***The views expressed on this web site/blog are mine alone and do not necessarily reflect the views of my employer, [insert name of Company employer].***"

F. Copyright & Trademarks

The Company retains the copyright to any material posted to any forum, newsgroup, chat, or web page by any User in the course of their employment duties. Company material posted in such a manner must be accompanied by appropriate claims for copyright as determined by the Company's Law Department. Except as necessary to perform his or her duties, and in the normal course of business, Users with internet access may not distribute data or software that is licensed or owned by the Company without approval from their manager and the proper IT manager.

G. Confidentiality

Users are reminded that chats, social media sites and newsgroups are public forums where it is wrong to disclose confidential business information of the Company (e.g., trade secrets, financial information, and customer data – See S.P.P. 1.0.2(IV)(F)) or belonging to a third party. Users releasing such confidential information - even if the release is accidental - will be subject to discipline in accordance with this and/or other existing Company policies and practices. Refer to SPP 1.0.2(IV)(U) for more information on Social Media use.

H. Security

No company data is to be saved or accessed on a personal device without prior approval. All Company data must be stored on a Company owned IT resource. Users must consider security with respect to all Company assets (i.e., computer, mobile device, and non-electronic documentation). This may include storing confidential paper records in locked drawers, using strong passwords, and safeguarding devices. Safeguarding devices includes using complex passwords, locking the device, and

physically securing the device when not in use. User IDs and passwords help maintain individual accountability for IT resource usage. Passwords should not be shared with any outside parties or co-workers. Executive Committee members may share passwords with assigned Administrative Assistants as needed if approved by the Chief Compliance Officer.

Attempting to circumvent the Company's IT security systems, compromising, or attempting to compromise the integrity of the IT Resource or using an IT resource without authorization or providing IT resources to individuals or groups without specific authorization is expressly forbidden.

I. News Services

In the interest of keeping Users well informed, use of news briefing services is acceptable within limits that may be set by the User's department management. Streaming of high-definition video should be utilized sparingly, as it consumes valuable bandwidth on Company systems.

J. Relevance to Other Policies

Company internet access and IT Resources used to intentionally commit infractions such as misusing Company assets or resources, sexual or other harassment, unauthorized public speaking, or stealing of intellectual property, among other unauthorized activity, are forbidden and will subject the User to discipline up to and including termination consistent with Company policies.

K. Purposeful Damage

No User may use the Company's internet facilities or any IT Resource to disable, hack, overload or avoid any computer system or network intended to protect the privacy or security of another User or another company. Any User who attempts to do so will be subject to immediate dismissal.

L. Personal Use of Company IT Resources

Provided that all above provisions are met, and the activity is lawful and in line with the Companies standards of conduct, Users may use Company-provided internet 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 and not utilize excessive bandwidth or storage capacity on Company computers, networks, or electronic storage media. Usage cannot compromise the security of the Companies IT Resources or company information and cannot be used for any personal financial gain. Files retained for personal use should, to the extent possible, be stored in a manner that does not consume Company IT Resources for back-up and retrieval of files. There is no expectation of privacy when using Company IT Resources, even for personal reasons.

Games and entertainment software determined to be virus vulnerable will be removed from IT Resources without notice. The IT Department is not responsible for recovering or maintaining music/movie files, personal pictures, or any other personal data on IT Resources.

M. Due Care

Users who receive e-mail may be exposed to malware 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 any file attachments. Users should maintain awareness of typical patterns displayed by e-mail viruses and should not

open attachments that could potentially corrupt the Company's computer systems. If a User receives an email and is uncertain whether it may contain malware, the User should report the receipt of the e-mail to the FS Service Desk at servicedesk@federalsignal.com, click on the outlook phishing button, or contact local IT personnel for further assistance.

It is required that all Users of the Company's IT resources go through IT Security training and remain aware of the Cybersecurity risks that can arise when utilizing those IT Resources. Spam/Phishing techniques are becoming increasingly sophisticated, and each User is responsible for ensuring that they complete required training, review all Cybersecurity alerts, and use best practices when utilizing the Company's IT Resources.

Users are expected to review all warnings from the Company about specific malware or viruses and are prohibited from opening/initiating potentially damaging e-mail attachments. Users are required to report the receipt of any suspicious e-mail to the FS Service Desk at servicedesk@federalsignal.com , click on the outlook phishing button, or contact local IT personnel for further assistance.

N. Monitoring and investigations

Any collection, access, use, transmission, or disposal of company information or use of company IT Resources, including personal use, may be audited, inspected, monitored, and/or investigated to:

1. Maintain, repair, and manage IT Resources for the efficient operation of the business systems,
2. Meet legal requirements to produce information, including litigation document discovery,
3. Ensure accessibility of Company IT Resources for the continuity of work processes,
4. Improve business processes and manage productivity, and
5. Ensure Compliance with legislative and policy requirements, including the Company's standards of conduct. Allegations of inappropriate access, collection, use, disclosure, or disposal of Company information or inappropriate use of Company IT Resources may be investigated, and investigations may include the search and/or seizure of IT Resources.

O. Alert and Notification

Users must immediately notify IT if they are aware of or suspect potential harm or risk to the network, or any Company IT Resource (i.e., account compromise, Cybersecurity attack, or phishing attempt).

Lost or stolen IT Resources must be reported immediately to the IT department and may be treated as a Cybersecurity event depending on the IT Resource. I If an IT Resource is stolen it is the User's responsibility to provide a police report to IT regarding the incident. If a Company owned mobile device like a cell phone is lost or stolen, or if the User's employment has been terminated, IT may wipe the device back to factory settings. If a personal or Company device used to access Company IT Resources is lost or stolen, or if the User's employment has been terminated, all Company data and applications will be promptly removed from the device.

IV. DISCLAIMER

Nothing in this SPP or any other Company policy or practice is designed to interfere with, restrain, or prevent User communications regarding wages, hours, or other terms and conditions of employment. Users have the right to engage in or refrain from such activities consistent with all legal requirements.

Any User consuming the Company's IT Resources that has been found to breach this policy will be subject to appropriate disciplinary procedures, including temporary or permanent loss of access privileges, and disciplined up to and including termination of employment.

V. DISTRIBUTION OF POLICY

This policy is to be read and understood by all Users of the Company who utilize the Company's computer, e-mail, or IT Resources. Managers and HR are to distribute this policy to all new Users and provide periodic reminders to all Users.