Federal Signal Corporation

Politiques et pratiques courantes

PSP n° 1.2.6

L'UTILISATION DU COURRIER ÉLECTRONIQUE, DES SERVICES D'ACCÈS À L'INTERNET ET DES RESSOURCES INFORMATIQUES FOURNIS PAR L'ENTREPRISE

I. OBJECTIF ET CHAMP D'APPLICATION

Établir une politique et des lignes directrices uniformes pour l'utilisation du courrier électronique de l'entreprise, de l'accès à Internet fourni par l'entreprise et de toutes les autres ressources des technologies de l'information ("TI"). Cette politique s'applique aux employés de l'entreprise, à ses utilisateurs et à ses sous-traitants, ainsi qu'à ses filiales nationales et étrangères (voir la définition de l'utilisateur ci-dessous).

Diverses autres politiques de l'entreprise s'appliquent à l'utilisation de l'internet par l'utilisateur, y compris, mais sans s'y limiter, celles qui traitent de la propriété intellectuelle, de la vie privée, de l'utilisation abusive des ressources informatiques de l'entreprise, du harcèlement sexuel et autre, des médias sociaux, de la sécurité des informations et des données, et de la confidentialité.

La connexion à l'internet peut présenter des risques importants pour les données et les systèmes de l'entreprise si un utilisateur ne respecte pas la discipline de sécurité appropriée. L'utilisation inutile ou non autorisée de l'internet provoque également un encombrement du réseau et des serveurs : elle ralentit les autres utilisateurs, réduit la productivité, consomme des ressources informatiques et sollicite inutilement d'autres systèmes partagés. Les données personnelles et les logiciels stockés sur les ressources informatiques consomment également les ressources informatiques disponibles et peuvent exposer l'entreprise à des plaintes en matière de propriété intellectuelle. L'utilisation inappropriée de données personnelles ou de l'internet peut également exposer l'entreprise à une publicité négative et à des responsabilités juridiques importantes. Chaque utilisateur est responsable de la gestion des informations de l'entreprise, ce qui inclut la protection des informations confidentielles et exclusives et la sauvegarde de la réputation de l'entreprise. Il est attendu des utilisateurs qu'ils fassent preuve d'un jugement sain et prudent et qu'ils agissent de manière éthique, en accord avec les valeurs de l'entreprise Federal Signal, lorsqu'ils utilisent les informations de l'entreprise :

1. Gestion de l'information sur les entreprises.
2. l'utilisation des ressources informatiques, que cette utilisation soit ou non liée à leurs fonctions professionnelles.
3. Utiliser les médias sociaux pour des raisons professionnelles ou personnelles de Federal Signal.

La Société autorise l'utilisation à des fins personnelles des ressources informatiques de la Société, sous réserve des limites raisonnables énumérées à la section III. L. du présent document.

L'Entreprise n'autorise pas le stockage ou l'accès à du matériel inapproprié, y compris du matériel au contenu illégal ou offensant (tel que défini dans le présent document). En outre, l'entreprise exige que les utilisateurs prennent les précautions prescrites dans le présent document et suivent une discipline raisonnable et appropriée en matière de sécurité. À aucun moment, une clé USB personnelle ne peut être utilisée pour stocker du matériel.

Il n'est pas permis de connecter un appareil de Federal Signal à un appareil appartenant à Federal Signal, y compris, mais sans s'y limiter, les ordinateurs, les ordinateurs portables, les appareils mobiles et les tablettes, sans l'autorisation de l'IT.

Tout utilisateur qui utilise une ressource informatique d'une manière qui cause sciemment ou soumet l'entreprise à une violation de la sécurité des données ou à la perte d'informations confidentielles de l'entreprise, ou qui viole sciemment la présente politique ou une politique connexe, s'expose à des mesures disciplinaires pouvant aller jusqu'à la résiliation du contrat de travail.

II. TERMES

Les termes suivants de la présente politique doivent être compris comme incluant des concepts connexes :

La "société" comprend Federal Signal Corporation et ses filiales nationales et étrangères ainsi que ses activités affiliées.

Le terme "document" désigne tout fichier ou site web pouvant être visualisé sur un écran d'ordinateur, y compris les courriers électroniques, les fichiers HTML lus dans un navigateur internet, tout fichier créé ou consulté par un traitement de texte, un tableur ou un programme de publication assistée par ordinateur ou son visualisateur, ou les fichiers préparés pour d'autres outils de publication électronique, tels que le lecteur Adobe Acrobat.

Par "ressource informatique", on entend tout équipement ou technologie virtuelle du département informatique, y compris, mais sans s'y limiter, les ordinateurs de bureau, les ordinateurs portables, les appareils mobiles fournis par l'entreprise tels que les téléphones cellulaires, les téléphones intelligents et les tablettes (y compris les iPads fournis par l'entreprise), les appareils de stockage de médias externes/amovibles tels que les disques durs externes et les clés USB, les ressources réseau, y compris les emplacements de stockage (lecteurs "personnels" ou lecteurs partagés par le service ou lecteurs partagés par des tiers comme OneDrive), les imprimantes et les scanners, les sites SharePoint, la vidéo en continu, les médias sociaux, l'accès au réseau et au VPN (réseau privé virtuel) et le courrier électronique, les systèmes et programmes logiciels de l'entreprise et l'accès à l'internet fourni par l'entreprise. Les identifiants, privilèges et accès délivrés par le département informatique doivent également être considérés comme des ressources informatiques.

Les **"graphiques**" comprennent les photographies, les images, les animations, les vidéos, les films ou les dessins.

"Le téléchargement est le processus de copie ou de transmission de fichiers ou de données à partir d'une source Internet ou d'un autre ordinateur vers l'ordinateur ou le réseau utilisé (généralement un ordinateur ou un réseau de l'entreprise). Cela inclut la récupération de fichiers joints à des messages électroniques.

Le terme **"malware**" est un terme générique désignant les logiciels conçus pour endommager, désactiver ou compromettre de toute autre manière un ordinateur ou un réseau d'appareils. Les exemples les plus courants sont les virus, les vers, les chevaux de Troie, les root kits, les ransomwares et les spywares.

Le terme "média" désigne tout support physique utilisé pour transférer ou distribuer des données numériques. Les exemples incluent les clés USB, les durs externes, les CD, les DVD et les appareils MP3.

Le "téléchargement" est le processus de copie ou de transmission de fichiers ou de données de l'ordinateur utilisé (généralement un ordinateur ou un réseau de l'entreprise) vers un autre ordinateur ou un autre réseau.

On entend par **"utilisateur"** toute personne, y compris, mais sans s'y limiter, les employés, les consultants et les vendeurs, qui a reçu l'autorisation d'accéder à une ressource informatique de l'entreprise.

III. DISPOSITIONS

A. Vie privée

L'entreprise se réserve le droit d'utiliser des logiciels et des systèmes pour surveiller et enregistrer tout le trafic Internet et de courrier électronique des utilisateurs et pour inspecter tous les fichiers stockés sur les ordinateurs, réseaux ou autres supports de stockage de l'entreprise afin de s'assurer que les ressources Internet de l'entreprise sont consacrées au maintien de la productivité et au respect des politiques de l'entreprise. Aucun utilisateur ne doit s'attendre à ce que son utilisation de l'internet, du courrier électronique, du chat ou de l'ordinateur sur les ressources de l'entreprise se fasse dans le respect de la vie privée.

B. Contenu offensant

L'affichage de tout type d'image ou de document sexuellement explicite sur une ressource informatique ou un système de l'entreprise constitue une violation de notre politique d'égalité des chances en matière d'emploi et est interdit. En outre, il est interdit d'accéder à ce type de matériel, de l'archiver, de le stocker, de le distribuer, de le visualiser, de l'éditer ou de l'enregistrer à l'aide des ressources informatiques de l'entreprise. L'accès à tout contenu offensant n'est pas autorisé sur les ressources informatiques de l'entreprise. L'entreprise peut utiliser des logiciels et des données fournis de manière indépendante pour identifier l'accès des utilisateurs à des sites Internet inappropriés ou sexuellement explicites. L'accès aux sites identifiés comme tels sera bloqué à l'intérieur de nos réseaux. Si un utilisateur se connecte accidentellement à un site contenant du matériel sexuellement explicite ou offensant, il doit se déconnecter immédiatement.

Les utilisateurs doivent contacter immédiatement leur responsable local des ressources humaines s'reçoivent un courriel, une pièce jointe ou un chat sexuellement explicite ou offensant.

C. Téléchargement de fichiers et de logiciels

Les utilisateurs disposant d'un accès à l'internet ne peuvent pas télécharger ou téléverser des fichiers ou des logiciels destinés à un usage illégal ou inapproprié et doivent prendre les dispositions nécessaires pour obtenir une licence et un enregistrement adéquats pour tout logiciel téléversé ou téléchargé et installé. Ces fichiers ou logiciels doivent être utilisés conformément à leur licence ou à leurs droits d'auteur. Tout programme téléchargé sur une ressource informatique de l'entreprise doit être approuvé par le service informatique.
Il n'est pas nécessaire d'obtenir l'approbation du service informatique pour ajouter des applications tierces aux smartphones et appareils similaires de l'entreprise si les applications sont obtenues légalement et conformes à la présente politique et aux autres politiques de l'entreprise. Tout logiciel ou fichier préapprouvé téléchargé ou téléversé sur les ressources informatiques de l'entreprise devient la propriété de l'entreprise. Le service informatique se réserve le droit de retirer un logiciel de l'équipement de l'entreprise sans en avertir l'utilisateur si ledit logiciel est jugé inapproprié, non autorisé, sans licence ou en violation de la présente politique ou d'une autre politique de l'entreprise. Pour cette raison, il est déconseillé aux utilisateurs d'utiliser des fichiers ou des logiciels personnels sur un ordinateur de l'entreprise, et il convient de faire preuve de prudence lors de l'utilisation d'applications sur les téléphones intelligents et autres appareils similaires de l'entreprise.

Les fichiers téléchargés à partir d'Internet ou d'autres sources externes doivent être analysés pour détecter les virus avant d'être utilisés. Le personnel d'assistance informatique de l'unité opérationnelle ou le service d'assistance informatique de l'entreprise peuvent apporter leur aide dans ce processus. Les utilisateurs doivent faire preuve de prudence et de bon sens et prendre les mesures appropriées pour s'assurer qu'ils n'utilisent pas le système Internet de l'entreprise pour propager un virus, un ver, un cheval de Troie ou un code de programme de trappe ou pour soumettre le système Internet de l'entreprise à de tels logiciels malveillants.

D. Utilisation licite

Les installations Internet et les ressources informatiques de la société doivent être utilisées conformément aux lois et réglementations des États-Unis et de tout pays dans lequel la société

maintient une présence commerciale, tout pays hébergeant un site web, et tout état, ville, province ou autre juridiction locale. Ces lois portent notamment sur les droits d'auteur, les marques commerciales, la responsabilité, la diffamation et le contrôle de la parole publique. L'utilisation intentionnelle de toute ressource informatique pour une activité illégale est un motif de licenciement immédiat, et l'entreprise coopérera avec toute enquête légitime des forces de l'ordre sur cette activité.

E. Représentation adéquate

Les utilisateurs et les sous-traitants doivent utiliser les comptes fournis par l'entreprise (par exemple, le courrier électronique) lorsqu'ils conduisent les affaires de l'entreprise. Les utilisateurs qui utilisent les installations Internet de l'entreprise doivent s'identifier honnêtement lorsqu'ils participent à des chats ou à des groupes de discussion, lorsqu'ils envoient des courriers électroniques ou lorsqu'ils créent des comptes sur des systèmes informatiques externes (tels que les médias sociaux ou les forums publics en ligne).

Seuls les utilisateurs autorisés peuvent parler ou écrire au nom de l'entreprise aux médias, aux analystes, aux réunions publiques, aux groupes de discussion ou aux forums de discussion. Un utilisateur autorisé est une personne qui a reçu l'autorisation préalable spécifique d'un responsable de l'entreprise à cette fin. Les utilisateurs autorisés doivent s'abstenir de tout soutien politique, de toute approbation ou apparence d'approbation par l'entreprise de tout produit ou service commercial non offert par l'entreprise, ses filiales ou ses sociétés affiliées.

Lorsqu'ils utilisent les ressources informatiques de l'entreprise et sauf autorisation de l'entreprise, les utilisateurs peuvent participer à des groupes de discussion ou à des chats, mais ils ne peuvent le faire qu'en leur nom propre. S'ils sont identifiés comme des utilisateurs de l'entreprise, ils doivent clairement indiquer que les opinions exprimées sont les leurs et non celles de l'entreprise en utilisant la clause de non-responsabilité suivante : "***Les opinions exprimées sur ce site web/blog sont les miennes uniquement et ne reflètent pas nécessairement celles de mon employeur, [insérer le nom de l'employeur de l'entreprise]***".

F. Droits d'auteur et marques

L'entreprise conserve les droits d'auteur sur tout matériel publié sur un forum, un groupe de discussion, un chat ou une page web par un utilisateur dans le cadre de ses fonctions. Le matériel de l'entreprise posté de cette manière doit être accompagné d'une demande de droits d'auteur appropriée, telle que déterminée par le service juridique de l'entreprise. Sauf dans la mesure nécessaire à l'exercice de ses fonctions et dans le cours normal de ses activités, l'utilisateur disposant d'un accès à l'internet ne peut distribuer des données ou des logiciels sous licence ou appartenant à l'entreprise sans l'autorisation de son supérieur hiérarchique et du responsable informatique compétent.

G. Confidentialité

Il est rappelé aux utilisateurs que les chats, les sites de médias sociaux et les groupes de discussion sont des forums publics où il est répréhensible de divulguer des informations commerciales confidentielles de l'entreprise (par exemple, des secrets commerciaux, des informations financières et des données sur les clients - voir S.P.P. 1.0.2(IV)(F)) ou appartenant à une tierce partie. Les utilisateurs qui divulguent de telles informations confidentielles - même si la divulgation est accidentelle - feront l'objet de mesures disciplinaires conformément à la présente politique et/ou à d'autres politiques et pratiques existantes de l'entreprise. Pour plus d'informations sur l'utilisation des médias sociaux, voir la section 1.0.2(IV)(U) des RPS.

H. Sécurité

Aucune donnée de l'entreprise ne doit être sauvegardée ou consultée sur un appareil personnel sans autorisation préalable. Toutes les données de l'entreprise doivent être stockées sur une ressource informatique appartenant à l'entreprise. Les utilisateurs doivent veiller à la sécurité de tous les actifs de l'entreprise (ordinateurs, appareils mobiles et documents non électroniques). Il peut s'agir de ranger les documents papier confidentiels dans des tiroirs verrouillés, d'utiliser des mots de passe forts et de protéger les appareils.
La protection des appareils comprend l'utilisation de mots de passe complexes, le verrouillage de l'appareil, et

sécuriser physiquement l'appareil lorsqu'il n'est pas utilisé. Les identifiants et les mots de passe permettent de maintenir la responsabilité individuelle dans l'utilisation des ressources informatiques. Les mots de passe ne doivent pas être partagés avec des tiers ou des collègues. Les membres du comité exécutif peuvent partager leurs mots de passe avec les assistants administratifs qui leur ont été attribués, si nécessaire, avec l'approbation du responsable de la conformité.

Il est expressément interdit de tenter de contourner les systèmes de sécurité informatique de l'entreprise, de compromettre ou de tenter de compromettre l'intégrité de la ressource informatique, d'utiliser une ressource informatique sans autorisation ou de fournir des ressources informatiques à des personnes ou à des groupes sans autorisation spécifique.

I. Services d'information

Afin de tenir les utilisateurs bien informés, l'utilisation de services d'information est acceptable dans les limites fixées par la direction du service de l'utilisateur. La diffusion en continu de vidéos haute définition doit être utilisée avec parcimonie, car elle consomme une bande passante précieuse sur les systèmes de l'entreprise.

J. Pertinence par rapport à d'autres politiques

L'accès à l'internet de l'entreprise et les ressources informatiques utilisées pour commettre intentionnellement des infractions telles que l'utilisation abusive des biens ou des ressources de l'entreprise, le harcèlement sexuel ou autre, la prise de parole en public non autorisée ou le vol de propriété intellectuelle, entre autres activités non autorisées, sont interdits et exposeront l'utilisateur à des mesures disciplinaires pouvant aller jusqu'au licenciement, conformément aux politiques de l'entreprise.

K. Dommages intentionnels

Aucun utilisateur ne peut utiliser les installations Internet de l'entreprise ou toute ressource informatique pour désactiver, pirater, surcharger ou éviter tout système ou réseau informatique destiné à protéger la vie privée ou la sécurité d'un autre utilisateur ou d'une autre entreprise. Tout utilisateur qui tenterait de le faire s'exposerait à un licenciement immédiat.

L. Utilisation personnelle des ressources informatiques de l'entreprise

Sous réserve que toutes les dispositions ci-dessus soient respectées et que l'activité soit légale et conforme aux normes de conduite de l'entreprise, les utilisateurs peuvent utiliser l'internet fourni par l'entreprise pour des recherches non professionnelles ou pour naviguer pendant les repas, les pauses ou en dehors des heures de travail.
L'utilisation doit rester dans des limites raisonnables déterminées par la direction de l'entreprise et ne pas utiliser une largeur de bande ou une capacité de stockage excessive sur les ordinateurs, les réseaux ou les supports de stockage électroniques de l'entreprise. L'utilisation ne doit pas compromettre la sécurité des ressources informatiques de l'entreprise ou des informations de l'entreprise et ne doit pas être utilisée à des fins de gain financier personnel. Les fichiers conservés à des fins personnelles doivent, dans la mesure du possible, être stockés de manière à ne pas utiliser les ressources informatiques de l'entreprise pour la sauvegarde et la récupération des fichiers. L'utilisation des ressources informatiques de l'entreprise, même à des fins personnelles, ne doit pas donner lieu à des attentes en matière de respect de la vie privée.

Les jeux et les logiciels de divertissement jugés vulnérables aux virus seront retirés des ressources informatiques sans préavis. Le département informatique n'est pas responsable de la récupération ou de la conservation des fichiers de musique ou de films, des photos personnelles ou de toute autre donnée personnelle sur les ressources informatiques.

M. La prudence est de mise

Les utilisateurs qui reçoivent des courriels peuvent être exposés à des logiciels malveillants causés par un expéditeur qui transmet, sciemment ou non, des courriels contenant des pièces jointes préjudiciables. Il est important de comprendre les risques liés à l'ouverture ou à l'exécution de tout fichier joint. Les utilisateurs doivent rester conscients des schémas typiques affichés par les virus de courrier électronique et ne doivent pas

ouvrir des pièces jointes susceptibles de corrompre les systèmes informatiques de l'entreprise. Si un utilisateur reçoit un courriel et n'est pas sûr qu'il contienne des logiciels malveillants, il doit signaler la réception du courriel au FS Service Desk à l'adresseservicedesk@federalsignal.com , cliquer sur le bouton outlook phishing ou contacter le personnel informatique local pour obtenir une assistance supplémentaire.

Tous les utilisateurs des ressources informatiques de l'entreprise doivent suivre une formation à la sécurité informatique et rester conscients des risques de cybersécurité qui peuvent survenir lors de l'utilisation de ces ressources informatiques. Les techniques de spam/phishing sont de plus en plus sophistiquées et il incombe à chaque utilisateur de s'assurer qu'il suit la formation requise, qu'il prend connaissance de toutes les alertes de cybersécurité et qu'il applique les meilleures pratiques lorsqu'il utilise les ressources informatiques de l'entreprise.

Les utilisateurs sont tenus de prendre connaissance de tous les avertissements de l'entreprise concernant des logiciels malveillants ou des virus spécifiques et il leur est interdit d'ouvrir ou d'initier l'envoi de pièces jointes potentiellement dommageables. Les utilisateurs sont tenus de signaler la réception de tout courriel suspect au FS Service Desk à l'adresseservicedesk@federalsignal.com , de cliquer sur le bouton outlook phishing ou de contacter le personnel informatique local pour obtenir une assistance supplémentaire.

N. Suivi et enquêtes

La collecte, l'accès, l'utilisation, la transmission ou l'élimination d'informations de l'entreprise ou l'utilisation des ressources informatiques de l'entreprise, y compris l'utilisation personnelle, peuvent faire l'objet d'un audit, d'une inspection, d'un contrôle et/ou d'une enquête :

1. Assurer la maintenance, la réparation et la gestion des ressources informatiques pour un fonctionnement efficace systèmes d'entreprise,
2. Satisfaire aux exigences légales en matière de production d'informations, y compris en ce qui concerne la recherche de documents dans le cadre d'un litige,
3. Assurer l'accessibilité des ressources informatiques de l'entreprise pour la continuité des processus de travail,
4. Améliorer les processus d'entreprise et gérer la productivité, et
5. Veiller au respect des exigences législatives et politiques, y compris les normes de conduite de l'entreprise. Les allégations d'accès, de collecte, d'utilisation, de divulgation ou d'élimination inappropriés d'informations de l'entreprise ou d'utilisation inappropriée des ressources informatiques de l'entreprise peuvent faire l'objet d'une enquête, qui peut inclure la fouille et/ou la saisie des ressources informatiques.

O. Alerte et notification

Les utilisateurs doivent immédiatement informer le service informatique s'ils ont connaissance ou s'ils soupçonnent un dommage ou un risque potentiel pour le réseau ou toute ressource informatique de l'entreprise (par exemple, compromission d'un compte, attaque de cybersécurité ou tentative d'hameçonnage).

Les ressources informatiques perdues ou volées doivent être immédiatement signalées au service informatique et peuvent être traitées comme un événement de cybersécurité en fonction de la ressource informatique. En cas de vol d'une ressource informatique, il incombe à l'utilisateur de fournir un rapport de police au service informatique concernant l'incident. En cas de perte ou de vol d'un appareil mobile appartenant à l'entreprise, tel qu'un téléphone portable, ou en cas de licenciement de l'utilisateur, le service informatique peut rétablir les paramètres d'usine de l'appareil. En cas de perte ou de vol d'un appareil personnel ou d'un appareil de l'entreprise utilisé pour accéder aux ressources informatiques de l'entreprise, ou en cas de licenciement de l'utilisateur, toutes les données et applications de l'entreprise seront rapidement supprimées de l'appareil.

IV. CLAUSE DE NON-RESPONSABILITÉ

Aucune disposition du présent PPS ou de toute autre politique ou pratique de l'entreprise n'est conçue pour interférer avec, restreindre ou empêcher les communications des utilisateurs concernant les salaires, les heures de travail ou d'autres conditions d'emploi. Les utilisateurs ont le droit de s'engager dans de telles activités ou de s'en abstenir, dans le respect de toutes les exigences légales.

Tout utilisateur des ressources informatiques de l'entreprise ayant enfreint la présente politique fera l'objet de procédures disciplinaires appropriées, y compris la perte temporaire ou permanente des privilèges d'accès, et de mesures disciplinaires pouvant aller jusqu'au licenciement.

V. RÉPARTITION DE LA POLITIQUE

Cette politique doit être lue et comprise par tous les utilisateurs de l'entreprise qui utilisent l'ordinateur, le courrier électronique ou les ressources informatiques de l'entreprise. Les responsables et les RH doivent distribuer cette politique à tous les nouveaux utilisateurs et faire des rappels périodiques à tous les utilisateurs.