Directive sur l'usage des moyens informatiques du Groupe PSA

Elle définit les règles d'utilisation du poste informatique et des moyens de communication mis à disposition des collaborateurs par l'entreprise. Ce document est destiné a être annexé au règlement intérieur de chaque entité juridique de GROUPE PSA utilisant les moyens fournis par la Direction des Systèmes d'Information du Groupe.

Préambule

L'essor des technologies de l'information et de la communication dans la vie de l'entreprise a modifié les modes de fonctionnement, d'échange et de transmission des informations professionnelles.

La présente directive a pour objet de définir les règles d'utilisation du poste informatique pour la protection des intérêts du Groupe et dans le respect des droits des utilisateurs. Ces règles doivent permettre à chaque utilisateur d'avoir en permanence à sa disposition un outil de travail efficace et sécurisé au bénéfice et pour la protection de l'entreprise.

En effet, l'utilisation de ces technologies doit respecter les exigences de disponibilité, de confidentialité et d'intégrité des informations traitées, l'image de l'entreprise ainsi que toutes les prescriptions légales et réglementaires applicables, en particulier celles qui concernent l'accès et l'utilisation des données personnelles.

Chaque utilisateur doit notamment utiliser les technologies de l'information et de la communication dans le cadre de la législation relative aux données personnelles, au respect des bonnes mœurs, de la dignité humaine, de la sensibilité et de l'image des personnes.

L'utilisation du poste informatique et de ses moyens de communication, propriété de GROUPE PSA, doit s'exercer dans le cadre de l'activité professionnelle. La messagerie électronique, le poste de travail ainsi que tous les matériels et logiciels qui sont fournis aux employés du Groupe sont destinés à un usage professionnel. Leur configuration, leur paramétrie et leur environnement sont susceptibles d'évoluer en fonction des besoins et des décisions du Groupe. En cas d'utilisation néanmoins pour des impératifs d'ordre privé, l'entreprise se réserve la possibilité de se retourner contre un utilisateur malveillant ou ayant porté atteinte à la protection des intérêts du Groupe.

Enfin, GROUPE PSA accepte la prise de parole liée à des thématiques du Groupe sur les réseaux sociaux et l'Internet, dans le respect des prescriptions en vigueur dans l'entreprise en matière de sécurité, de confidentialité, d'usage et de responsabilité personnelle de l'utilisateur. Cette participation devant en outre rester ponctuelle, raisonnable et ne pas affecter l'activité professionnelle de l'utilisateur.

Cette directive s'applique à tout utilisateur de poste informatique ou d'accès aux réseaux et applications informatiques du Groupe qu'il soit salarié ou non de GROUPE PSA.

I. Le poste informatique

Le poste informatique comprend l'ensemble des moyens informatiques (poste de travail, périphériques et logiciels installés) mis à la disposition des utilisateurs par GROUPE PSA pour l'exécution de leurs missions professionnelles et s'étend aux accès autorisés aux espaces de travail en ligne, à la messagerie, au réseau Intranet ou à l'Internet et les applications et fichiers informatiques de GROUPE PSA.

I.1 Poste de travail

Le poste informatique est mis à disposition d'un utilisateur par GROUPE PSA. Cette configuration matérielle ne peut être modifiée sans accord de la Direction des Systèmes d'Information.

Les activités du Groupe seront réalisées exclusivement sur les matériels affectés à l'employé chaque fois que cela est possible.

I.2 La messagerie

Les utilisateurs d'un accès à la messagerie disposent d'une adresse électronique nominative leur permettant d'échanger et de transmettre des informations de nature professionnelle avec leurs interlocuteurs tant internes qu'externes à GROUPE PSA.

Chaque collaborateur veille à n'engager l'entreprise par le contenu d'un mail que conformément à sa lettre de mission.

Les utilisateurs disposent aussi d'une fonctionnalité de messagerie instantanée, utilisable uniquement depuis le réseau du GROUPE PSA. Les utilisateurs sont libres de gérer leur disponibilité/joignabilité dans cet outil.

La confidentialité des transmissions n'étant jamais assurée, les utilisateurs doivent limiter l'envoi d'informations à caractère sensible ou confidentiel à l'extérieur de GROUPE PSA aux nécessités de leur mission professionnelle conformément à la Directive Groupe « Maîtrise de l'Information - Confidentialité ». Des outils de chiffrement sont mis à leur disposition dans le cas d'informations confidentielles.

Les mails doivent comporter leur niveau de confidentialité : les mentions NON SENSIBLE, SENSIBLE PSA, CONFIDENTIEL PSA doivent alors être ajoutées en début de message.

Le niveau de confidentialité SECRET PSA ne peut pas être utilisé dans la messagerie électronique.

Les moyens de stockage et de protection doivent être adaptés à leur niveau de confidentialité : les messages classifiés CONFIDENTIEL doivent être chiffrés avec les moyens techniques fournis par le Groupe.

Il est interdit de faire suivre automatiquement (Forward) les messages reçus à titre professionnel vers une adresse de messagerie qui n'est pas sous le contrôle exclusif de GROUPE PSA.

Les utilisateurs doivent respecter la destination professionnelle de cet outil de travail. En cas d'utilisation néanmoins pour des impératifs d'ordre privé, l'entreprise se réserve la possibilité de se retourner contre un utilisateur malveillant ou ayant porté atteinte à la protection des intérêts du Groupe.

Elle s'effectuera conformément aux prescriptions légales et réglementaires applicables en matière de sécurité, de confidentialité, d'image et de responsabilité personnelle de l'utilisateur

Il est interdit d'utiliser la messagerie professionnelle mise à disposition par GROUPE PSA pour véhiculer ou échanger des propos discriminants, xénophobes, sexistes, homophobes, pédophiles ou racistes.

GROUPE PSA se réserve le droit de procéder à des contrôles et investigations dans les conditions décrites au sein de la partie III de la présente directive pour s'assurer du respect des règles rappelées ci-dessus.

I.3 Le réseau Intranet

Tout utilisateur disposant d'un poste informatique connecté au RPI (Réseau de Postes Informatiques) a un accès au réseau Intranet de GROUPE PSA. Ce réseau permet aux utilisateurs d'accéder aux sites, services et applications développés par les différentes Directions en vue de s'informer ou de collaborer à certaines missions de GROUPE PSA.

Pour des raisons de confidentialité, l'accès à certains sites, services et applications est réservé au personnel autorisé.

Il appartient à l'utilisateur de s'assurer qu'il entre dans son champ de compétence professionnel de publier des informations sur ces sites, services et applications en veillant au respect du niveau de confidentialité requis des informations ainsi publiées.

Il est interdit au personnel non autorisé nominativement de tenter de pénétrer ou de pénétrer dans des parties sécurisées du réseau, dans des serveurs sécurisés ou dans les fichiers d'un utilisateur.

I.4 L'Internet

Tous les utilisateurs dotés d'un accès RPI bénéficient d'un accès à certains sites d'intérêt général.

Une partie des utilisateurs bénéficient d'un accès individuel à l'Internet sur décision de leur Direction.

L'usage qui est fait de cet accès doit rester conforme à sa destination professionnelle. Cet accès peut être retiré à tout moment, notamment en cas d'utilisation non conforme.

Dans ce cadre :

- GROUPE PSA tolère une utilisation personnelle, ponctuelle, raisonnable et limitée de l'accès l'Internet dans le cadre des strictes nécessités de la vie privée, à condition qu'elle n'affecte pas

l'activité professionnelle. Cette utilisation doit rester exceptionnelle et limitée et s'effectuera conformément aux prescriptions légales et réglementaires applicables en matière de sécurité, de confidentialité, d'usage et de responsabilité personnelle de l'utilisateur.

- GROUPE PSA accepte la prise de parole liée à des thématiques du Groupe sur les réseaux sociaux et l'Internet. Cette prise de parole est de la responsabilité personnelle de l'utilisateur. Elle est soumise au respect des prescriptions en vigueur dans l'entreprise en matière de sécurité, de confidentialité, d'usage et de responsabilité personnelle de l'utilisateur. Cette participation aux réseaux sociaux doit rester ponctuelle, raisonnable et ne pas affecter l'activité professionnelle de l'utilisateur.

Dans tous les cas il est interdit d'utiliser le poste informatique mis à disposition par GROUPE PSA pour :

- se connecter à des sites pénalement sanctionnables, notamment xénophobes, sexistes, homophobes, pédophiles ou racistes.
- véhiculer ou échanger sur l'Internet des propos diffamatoires ou discriminants, notamment xénophobes, sexistes, homophobes, pédophiles ou racistes.
- adopter des comportements susceptibles de nuire au Groupe en termes de sécurité informatique, d'image, de confidentialité des données, de contenus publiés.

Il est rappelé que l'utilisateur doit, dans tous les cas, veiller au respect de ses obligations de confidentialité, de loyauté et de discrétion à chaque fois qu'il fait usage de son accès à l'Internet fourni par le Groupe que ce soit pendant ou hors de son temps de travail et plus particulièrement, à chaque fois qu'il participe à des échanges liés au Groupe et à ses produits sur l'Internet.

Les conseils de bon usage pour participer à des discussions sur les réseaux sociaux sont disponibles sur l'intranet du Groupe http://protection.inetpsa.com .

GROUPE PSA se réserve le droit de procéder à des contrôles et investigations dans les conditions décrites au sein de la partie III de la présente directive pour s'assurer du respect des règles rappelées ci-dessus.

I.5 Les logiciels et fichiers informatiques

Le poste informatique est doté de logiciels sélectionnés par l'entreprise pour leur compatibilité entre eux ainsi que pour leur capacité à répondre aux besoins de chaque utilisateur dans l'accomplissement de ses missions.

Pour ces raisons, les utilisateurs ne sont autorisés à sauvegarder, installer, importer ou modifier des logiciels sur leur poste informatique qu'après accord de la Direction des Systèmes d'Information.

Par ailleurs, les utilisateurs ne sont autorisés à importer, envoyer ou diffuser des fichiers, qu'à la condition que ces opérations soient réalisées dans le cadre de leurs activités professionnelles et en utilisant les moyens professionnels mis à leur disposition par le Groupe

L'enregistrement et le traitement de Données à Caractère Personnel (DCP) sur le poste de travail informatique doivent rester exceptionnels. Ils ne sont tolérés que pour répondre à des besoins essentiels de l'entreprise quand aucune autre solution n'est possible. Ils doivent être limités dans le temps et les données doivent être protégées conformément à la politique de protection des données du Groupe PSA.

Aucune tolérance ne sera admise quant à la présence sur le poste informatique de logiciels et fichiers informatiques ayant un contenu discriminant, xénophobe, sexiste, homophobe, pédophile ou raciste.

GROUPE PSA se réserve le droit de procéder à des contrôles et investigations dans les conditions décrites au sein de la partie III de la présente directive pour s'assurer du respect des règles rappelées ci-dessus.

II. La sécurité des systèmes d'information

L'utilisateur doit respecter les dispositions de sécurité mises en place sur son poste de travail ou dans des systèmes distants (règles d'accès, pare feu, antivirus, filtres, …) et ne pas chercher à les contourner par quelque moyen que ce soit.

L'utilisation de moyens personnels est à proscrire chaque fois qu'une solution sous le contrôle du Groupe est disponible. Lorsqu'un moyen personnel est utilisé sur un site PSA, seule la connexion au réseau informatique « WiFi guest » est autorisée.

L'hébergement d'informations professionnelles par des services extérieurs au Groupe est interdit sauf accord de la Direction de la Sûreté Groupe.

L'utilisation de moyens amovibles d'échange d'informations (type clés USB, disque externe…) est à proscrire chaque fois que possible en utilisant les moyens préconisés par le Groupe.

II.1 Identification et authentification

Plusieurs mots de passe ou certificats électroniques sont susceptibles d'être utilisés par un utilisateur selon les moyens techniques mis en œuvre (RPI, messagerie, etc.).

Un mot de passe et un certificat sont strictement personnels et confidentiels parce qu'ils authentifient l'identifiant présenté. Le mot de passe et le certificat étant personnels, la responsabilité du titulaire sera recherchée lors des accès effectués avec le mot de passe, le certificat, et son identifiant.

Pour des raisons de sécurité, il est demandé à l'utilisateur de choisir des mots de passe difficilement devinables par d'autres que lui. Des préconisations pour construire des mots de passe robustes et les mémoriser sont disponibles sur le site My IT Portal.

Pour ces mêmes raisons de sécurité, il est également demandé à l'utilisateur de veiller à verrouiller son poste informatique lorsqu'il s'absente momentanément de son poste au cours de la journée et en fin de journée.

II.2 Mise à jour du poste informatique

L'utilisateur doit veiller à mettre systématiquement à jour son poste informatique. Dès qu'il est informé par une notification visuelle sur son poste qu'une nouvelle version est disponible, il doit exécuter la montée de version

La mise à jour garantit à l'utilisateur d'avoir un poste informatique bénéficiant des dernières évolutions logicielles et disposant du meilleur niveau de protection. Le fonctionnement de l'antivirus ne doit pas être désactivé par l'utilisateur.

II.3 La prise de vue

Dans le cadre de la maîtrise des informations, les prises de vues à l'intérieur du site sont interdites, sauf accord spécifique de la Direction du site.

Sont concernées les fonctions de prise de vue de tout appareil permettant la prise de vues fixes ou animées (exemples : appareils photo, caméscope, téléphones ou assistants personnels portables, micro-ordinateurs, …).

II.4 Bonnes pratiques

L'utilisateur est tenu de respecter les « 10 Bonnes Pratiques de la Cyber-sécurité » publiées dans le Référentiel du Groupe et accessibles via le site de la Protection du Groupe http://protection.inetpsa.com

III. L'analyse et le contrôle d'utilisation

III.1 Principe général

Dans le respect de la législation applicable, GROUPE PSA se réserve le droit de procéder à des contrôles et investigations pour s'assurer du respect des règles édictées dans la présente directive.

Les dispositifs de surveillance qui mettent en œuvre un traitement de données à caractère personnel, peuvent faire l'objet d'une déclaration auprès des organismes ou autorités compétentes en fonction de la règlementation du pays concerné (ex : le RGPD en Europe ; la CNIL en France).

GROUPE PSA pourra sonder et examiner la nature des informations circulant sur ses réseaux et sur les matériels qu'il met à disposition de ses collaborateurs

En présence d'indices révélant une utilisation de postes informatiques ou de moyens de communication non conformes aux dispositions de cette directive, l'entreprise pourra procéder à l'examen détaillé du contenu des informations et logiciels présents sur les postes informatiques. Ces informations étant présumées avoir un caractère professionnel, leur contrôle pourra être effectué hors la présence du salarié sauf dans les cas où elles auront été explicitement identifiées par lui comme personnelles. Dans ce dernier cas, le contrôle se fera en présence de l'utilisateur sauf risque ou événement particulier.

En cas de non conformités constatées, une procédure disciplinaire pourra être engagée à l'encontre de l'utilisateur concerné.

III.2 Mise en œuvre pratique

Messagerie :

Le contrôle est opéré dans les infrastructures centrales de la messagerie. Les informations enregistrées lors de l'envoi de messages sont les suivantes : identification de l'émetteur, date et heure, adresse IP (Internet Protocol) du poste informatique, adresse mail du ou des destinataires, volume échangé et nature de la pièce jointe le cas échéant. L'utilisateur est averti qu'elles sont conservées sur une durée de douze mois glissants.

Pour la fonction « messagerie instantanée », les informations enregistrées lors de l'envoi de messages sont les suivantes : identification de l'émetteur, date et heure, adresse IP (Internet Protocol) du poste informatique, identification du ou destinataire, volume échangé et nature de la pièce jointe le cas échéant ; ces informations sont conservées 90 jours.

L'Internet :

Le contrôle est opéré dans les infrastructures centrales d'accès à l'Internet. Les informations enregistrées sont les suivantes : identifiant, date, heure, adresse IP (Internet Protocol) du poste informatique, nom du serveur destinataire, volume échangé et nature de l'échange. L'utilisateur est averti qu'elles sont conservées sur une durée de douze mois glissants.

Le poste informatique, les logiciels et les fichiers :

Le contrôle est opéré dans les infrastructures centrales de gestion des postes de travail. Il porte sur la détection de logiciels dangereux, associée au processus de lutte contre les virus et sur la gestion des licences logicielles acquises ou louées par le Groupe. En cas de besoin, une intervention est opérée directement sur les postes de travail, selon les modalités visées au paragraphe III.1 et conformément à la Directive Groupe« Accès au poste de travail utilisateur »

IV. Les interlocuteurs de l'utilisateur

IV.1 L'Administrateur de Sécurité Logique (ASL)

Il est l'interlocuteur unique de l'utilisateur en ce qui concerne les aspects liés à la sécurité et notamment : fourniture et dépannage des moyens d'authentification (mot de passe, certificats électroniques, etc.), attribution des droits d'accès au juste nécessaire aux systèmes d'information du Groupe.

IV.2 Le support local au poste (SLP)

Il est à la disposition des utilisateurs pour les aider et les renseigner sur le fonctionnement du poste informatique.

Il est le garant de la gestion des logiciels : il coordonne les montées de versions et valide les demandes de logiciels faites par les utilisateurs.

IV.3 Le Responsable de Direction pour la Maîtrise de l'Information (RDMI)

Il est l'interlocuteur unique de l'utilisateur en ce qui concerne les aspects liés à la sûreté et notamment les questions de gouvernance et de bonnes pratiques

IV.4 La Direction en charge de la communication et les équipes de communication locales

Garante de l'image et de la réputation du Groupe, elle est à disposition des utilisateurs qui se posent des questions sur la prise de parole sur l'Internet.

IV.5 La Direction en charge des Systèmes d'Information

Est en charge de la définition et de la configuration des moyens informatiques pour en garantir la protection et la sécurité.

IV.6 La Direction en charge de la Sûreté Groupe

Est en charge de la Gouvernance de la Sécurité du Groupe PSA. Elle est garante de la définition et de l'application des règles de sécurité applicables par les utilisateurs et par les systèmes d'informations

V. Responsabilité et sanctions

Le non-respect des règles définies dans la présente directive pourra notamment entraîner des sanctions conformément à l'échelle des sanctions disciplinaires prévue par le Règlement Intérieur en vigueur dans l'établissement d'affectation de l'utilisateur.

La responsabilité de l'utilisateur d'un poste informatique pourra être recherchée pour toutes les conséquences judiciaires pouvant résulter d'actes commis au moyen des outils et des accès informatiques du Groupe.

VI. Dispositions finales

Les dénominations hiérarchiques ou fonctionnelles ainsi que les appellations techniques sont susceptibles d'être modifiées dans le temps.

Ces changements de dénominations ou d'appellations ne sauraient modifier les règles et principes édictés par la présente directive.

La présente directive entre en vigueur le 1er janvier 2021.

VII. Documents de référence

Politique Groupe Sûreté de l'Information : DocInfo ref.01249_19_00067

Politique Groupe Protection des Données : Docinfo ref.01989_18_00268