Annexe 1 :

Postes identifiés à risques dans le règlement intérieur :

- Postes nécessitant la manipulation d'agents chimiques dangereux, ou l'utilisation des machines-outils;

- Postes nécessitant l'utilisation d'engins autoportés, nacelles, transpalettes électriques quel que soit le périmètre ;

- Postes nécessitant un travail en hauteur ;

- Postes nécessitant l'utilisation de véhicules pour l'exercice de la mission du collaborateur.

Annexe 2

Charte d'utilisation des systèmes d'information et de communication

PREAMBULE

Objet de la Charte

La présente charte, annexée au règlement intérieur, définit les conditions générales d'utilisation du Système d'Information et de Communication mis à la disposition des Utilisateurs par l'Entreprise.

Dans un but de transparence, de promotion d'une utilisation loyale, responsable et sécurisée du Système d'Information, cette charte vise à sensibiliser les Utilisateurs et à attirer leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'Entreprise. Elle définit pour cela les règles de bonnes pratiques que les Utilisateurs et l'Entreprise s'engagent à appliquer, et précise les droits et devoirs de chacun, dans le respect de la législation applicable.

Définitions

Administrateur : On désigne par le terme « administrateur » toute personne physique ayant la responsabilité technique du bon fonctionnement de l'une des Ressources du Système d'Information de l'Entreprise.

Confidentialité : La confidentialité est définie comme « le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé ». C'est une propriété de sécurité visant par conséquent à se prémunir contre l'accès ou la divulgation non autorisé de l'information.
Les informations de l'Entreprise sont classées suivant 4 niveaux de confidentialité : publique, société, confidentiel, secret.

Correspondant sécurité : On désigne sous le terme de « correspondant sécurité » une personne physique désignée par l'Entreprise pour être l'interlocuteur privilégié sensibilisé aux problèmes de sécurité.

Disponibilité : La disponibilité vise à assurer la prévention contre l'utilisation illégale ou abusive des Ressources et des services offerts par le Système d'Information.

Données à caractère personnel : par données à caractère personnel, il faut entendre toute information relative à une personne physique pouvant être identifiée directement ou indirectement, par référence à un numéro d'identification (numéro de sécurité sociale, matricule, etc...), ou un ou plusieurs éléments qui lui sont propres (nom, date de naissance, verbatim, données biométriques, etc...). Certaines données, dites « sensibles » (origines sociales ou ethniques, opinions politiques, philosophiques ou religieuses ou appartenance à un syndicat, données relatives à la santé ou la vie sexuelle), sont soumises à autorisation.

Entreprise : On désigne par le terme « Entreprise » tous les établissements appartenant à Auchan France.

Intégrité : L'intégrité consiste à protéger une information ou un système contre une altération ou une destruction non autorisée.

Internet : Système mondial d'interconnexion de réseaux informatiques permettant l'échange d'informations entre des ordinateurs au moyen d'applications et de services variés comme le courrier électronique, la messagerie instantanée et le World Wide Web.

Intranet : L'Intranet est un ensemble de moyens informatiques utilisant les techniques de communication standardisées de l'Internet, mais dont l'accès est limité à l'intérieur de l'Entreprise et de ses Utilisateurs.

Plateforme : On désigne par le terme « Plateforme », le réseau communautaire et collaboratif mis à la disposition des collaborateurs de l'Entreprise afin de faciliter la conduite de projets professionnels en commun et de promouvoir la communication entre les différents utilisateurs bénéficiant d'un accès autorisé, au sens des conditions générales d'utilisation.

Ressource : Une « ressource » est le terme générique employé pour désigner tous les moyens informatiques centraux ou locaux, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau du site.
Site : On désigne sous le terme « site » les établissements utilisés par l'Entreprise pour l'accomplissement de ses missions.

Système d'Information (ou SI) : On entend par « Système d'Information » l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications pouvant être mis à disposition de l'Utilisateur par l'Entreprise. Ces moyens englobent notamment :

les équipements informatiques et de communication fixes et nomades : ordinateurs portables, stations de travail, serveurs, tablets PC, téléphones fixes et mobiles, smartphones & assistants personnels, télécopieurs, périphériques, imprimantes ;
les moyens de communication et de collaboration : système de messageries électronique et instantanée, Intranet et Plateforme, lignes téléphoniques fixes & mobiles, accès Internet ;
les informations, les bases de données et les données.

Pour des raisons de sécurité, est également considéré comme faisant partie du SI, le réseau, le matériel personnel des salariés connecté au réseau de l'Entreprise ou contenant des informations à caractère professionnel

La composition du SI est indifférente à la propriété des éléments qui le composent.

Traitement de données : par traitement de données, il faut entendre, toute opération de collecte, enregistrement, organisation, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion, ou toute autre forme de mise à disposition, rapprochement, interconnexion, verrouillage, effacement, destruction. Le traitement concerne aussi bien les fichiers automatisés que les fichiers manuels.

Utilisateur : On désigne par le terme « Utilisateur » toute personne physique ayant accès ou utilisant les Ressources du Système d'Information dans le cadre de l'exercice de son activité professionnelle. Est ainsi considéré comme Utilisateur toute personne travaillant au service de l'Entreprise, quel que soit son statut et/ou son contrat : dirigeant, salarié à temps plein ou temps partiel, personnel intérimaire, stagiaire, ainsi que tout prestataire externe ayant contracté avec l'Entreprise.

ARTICLE 1 : CHAMP D'APPLICATION

La présente charte s'applique à l'ensemble des Utilisateurs(1) du Système d'Information de l'Entreprise(2).

1 Tel que défini dans le préambule
2 Telle que définie dans le préambule

La sécurité est la responsabilité de chacun.

Chaque Utilisateur du Système d'Information doit y contribuer en s'engageant à connaître et à respecter les bonnes pratiques décrites dans la présente charte.

ARTICLE 2 : PRINCIPES GENERAUX DE SECURITE

2.1. Modalités d'accès aux Ressources

L'Entreprise met en œuvre des mécanismes de protection appropriés sur les Systèmes d'Information mis à disposition des Utilisateurs. En particulier, une politique globale de contrôle d'accès est définie pour maîtriser l'accès au patrimoine informationnel sensible de l'Entreprise.

Chaque Utilisateur, après autorisation préalable de l'Entreprise, dispose d'un accès strictement personnel au Système d'Information. Cet accès et tout usage du Système d'Information ne peut être cédé à quiconque, temporairement ou définitivement. Les moyens d'accès au Système d'Information (clef, badge magnétique, code, mot de passe, etc.) seront remis par l'Entreprise et seront associés à des moyens d'identification et de contrôle de l'usage qui en est fait. Le cas échéant, une attestation de remise des moyens d'accès (clef, badge magnétique, code, mot de passe, etc.) est signé en deux exemplaires par l'Entreprise et l'Utilisateur concerné. En toute hypothèse, l'Entreprise reste et demeure seul décisionnaire et à tout moment quant à l'accès et à l'usage accordé ainsi que l'unique propriétaire desdits moyens d'accès mis à disposition.

Les codes d'accès servent à identifier l'Utilisateur, ainsi que les actions qu'il entreprend sur le Système d'Information. Chaque code d'accès (mot de passe, code PIN d'un badge, digicode pour les accès physiques, etc.) constitue ainsi une mesure de sécurité permettant de protéger les données et les outils contre toute utilisation malveillante ou abusive. Leur efficacité n'est garantie que si l'Utilisateur s'impose de :

- respecter les consignes de sécurité, notamment les règles relatives à la création et au renouvellement des mots de passe,
- garder strictement confidentiel son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers, ni le(s) prêter,
- respecter les règles de gestion des accès, en particulier ne pas utiliser les identifiants et mots de passe d'un autre Utilisateur, ni chercher à les connaître.

L'Utilisateur est informé qu'en cas de suspension du contrat de travail, de dispense d'activité, et/ou de rupture du contrat de travail pour quelque motif ou quelque cause que ce soit, l'Entreprise pourra, selon le cas et les circonstances, être amenée, à restreindre, suspendre ou supprimer l'accès aux Ressources, temporairement ou définitivement, afin notamment de préserver la sécurité du Système d'Information.

La mise en œuvre d'une telle mesure s'effectuera :

- sauf impossibilité ou circonstances particulières, avec information de l'Utilisateur,
- de telle sorte qu'elle n'aura pas pour effet d'entraver l'exercice des mandats électifs, désignatifs ou représentatifs que possèderait l'Utilisateur.

2.2. Règles générales d'usage

Pour optimiser la sécurité des Ressources mises à disposition de l'Utilisateur, il est nécessaire de respecter les règles générales d'usage suivantes :

- porter en toutes circonstances et de manière apparente son badge d'identification nominatif dans les locaux de l'Entreprise ;
- ne pas utiliser les Ressources qui sont offertes pour proposer ou rendre accessible à des tiers des informations, sensibles, stratégiques, confidentielles ou contraires à la législation en vigueur ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'Entreprise, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
- ne pas mettre en place des moyens de prise de main ou de contrôle d'équipement interne au Système d'information depuis Internet
- ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau de l'Entreprise des logiciels sans lien avec l'activité professionnel. Il est par ailleurs strictement interdit d'installer, de télécharger ou d'utiliser des logiciels dont les droits de licence n'ont pas été acquittés ou ne provenant pas de sites dignes de confiance ; Une vigilance particulière sera portée au fait qu'un téléchargement d'un logiciel dont la licence est gratuite à titre privé peut ne pas l'être dans le contexte de l'Entreprise
- ne pas apporter volontairement des perturbations au bon fonctionnement des Ressources informatiques et des réseaux de communication ; D'une façon générale, hormis particularité professionnelle, il n'est pas autorisé de regarder les chaines de TV, les émissions en streaming ou d'écouter la radio sur le web
- Se conformer aux dispositifs mis en place par l'Entreprise pour lutter contre les virus et autres programmes malveillants ; Ne pas modifier ou désactiver les mécanismes de protection (antivirus, paramétrage des mots de passe, installation des correctifs de sécurité...).
- assurer l'identification de ses informations suivant la classification en vigueur dans l'Entreprise : publique, société, confidentiel, secret. Utiliser les différents moyens mis à sa disposition par l'Entreprise pour les protéger : règles de nommage, outils de chiffrement de données, moyens de sauvegarde individuels et collectifs. En particulier, l'Utilisateur doit veiller à protéger ces informations lorsqu'elles sont stockées sur des supports non fiables, tels que ordinateurs portables, smartphones, clés USB, DVD, disques externes, etc. ;
- enregistrer les documents contenant des informations de l'Entreprise conformément aux règles de classification des informations et de gestion des connaissances afin d'éviter toute perte du patrimoine informationnel de l'Entreprise ;
- identifier explicitement les données créées (fichiers, courriers électroniques, etc.) conformément à leur objet réel ;
- ne pas quitter son poste de travail, ni ceux en libre-service, en laissant des Ressources ou services accessibles, et ce, en verrouillant systématiquement la session Utilisateur ;
- fermer systématiquement la session Utilisateur à l'issue de sa journée de travail et/ou le cas échéant, se déconnecter de la Plateforme en fin d'utilisation, afin de préserver l'accès aux Ressources et la sécurité du Système d'Information de l'Entreprise ;

- coopérer si besoin avec le service informatique, et plus particulièrement l'Administrateur et le Correspondant sécurité, et le cas échéant, effectuer toutes opérations notamment de maintenance et de mise à jour locales qui s'avèreraient nécessaires pour préserver la sécurité et le bon fonctionnement du Système d'Information.

  Il signale le plus rapidement possible à son service informatique toute perte ou vol d'un équipement mis à sa disposition

2.3. Mesures de contrôle de la sécurité

L'Utilisateur est informé que :

pour effectuer la maintenance corrective, curative ou évolutive, l'Entreprise se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les Ressources mises à sa disposition ;
une maintenance à distance est précédée d'une information de l'Utilisateur ;
le Système d'Information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de non-respect de la Charte Informatique et notamment de détection des abus.

Les Administrateurs, en charge des opérations de contrôle, sont soumis au secret professionnel. Ils ne peuvent donc pas divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction dès lors que :

ces informations sont couvertes par le secret des correspondances ou, qu'elles relèvent de la vie privée de l'Utilisateur parce qu'elles sont identifiées comme telles ;
elles ne mettent en cause ni le respect de la Charte Informatique, ni le bon fonctionnement technique du Système d'Information et de ses Ressources, ni leur sécurité.

ARTICLE 3 : CONDITIONS GENERALES D'UTILISATION DES RESSOURCES

3.1. Utilisation professionnelle / privée des Ressources

Chaque Utilisateur contribue à la sécurité du Système d'Information par la maîtrise de l'usage qu'il fait des Ressources auxquelles il a le droit d'accéder. A ce titre, il doit avoir conscience que l'usage des Ressources obéit à des règles qui s'inscrivent dans le respect :

de la loi applicable,
des recommandations de bon usage, gage d'efficacité opérationnelle,
de la sécurité de l'Entreprise dans son ensemble.

L'Utilisateur doit réserver l'usage de ces Ressources au cadre de son activité professionnelle. Un usage personnel occasionnel et modéré des Ressources est toléré dans le cadre des nécessités de la vie courante et familiale. Il ne doit cependant pas entraver la bonne exécution du contrat de travail ou de la mission et, en aucun cas, nuire à l'intérêt de l'Entreprise, de ses clients ou de ses collaborateurs.
Toute information stockée sur les Systèmes d'Information de l'Entreprise est réputée professionnelle et peut être consultée par l'Entreprise, à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie privée.
Ainsi, il appartient à l'Utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu à cet effet et d'en indiquer expressément le caractère personnel.
L'Utilisateur est responsable de la gestion de son espace de données à caractère personnel. La sauvegarde régulière de ces données, ainsi que leur suppression (lors d'un départ définitif), relèvent de l'entière responsabilité de l'Utilisateur.

3.2. Respect du droit de propriété intellectuelle

Toute œuvre de l'esprit (3) produite par l'Utilisateur dans le cadre de sa mission est la propriété de l'Entreprise et le demeure sans limitation de temps. Certaines informations considérées comme sensibles ou stratégiques font partie intégrante du savoir-faire de l'Entreprise et doivent être tenues confidentielles conformément aux règles de classification des informations et de gestion des connaissances.

(3) Ceci inclut les logiciels, bases de données, pages Web, textes, sons, images, photographies, vidéo, etc.

L'Utilisateur ne doit pas reproduire, copier, diffuser, modifier ou utiliser les œuvres de l'esprit protégées par le droit d'auteur ou un droit de propriété intellectuelle, sans avoir obtenu le consentement préalable des titulaires de ces droits. Notamment, les Utilisateurs sont pleinement tenus par les conditions générales d'utilisation de la Plateforme concernant les contributions qu'ils publient.

Par ailleurs, il est strictement interdit d'effectuer des copies de logiciels commerciaux et données mis à disposition de l'Utilisateur par l'Entreprise. Les copies de sauvegarde, dans les conditions prévues par le code de la propriété intellectuelle, ne peuvent être effectuées que par les personnes habilitées. Le téléchargement ou la copie d'un logiciel, ou de toute œuvre de l'esprit, en violation des droits de l'auteur constitue un délit de contrefaçon. L'auteur d'un acte de contrefaçon engage directement sa responsabilité. Il peut être poursuivi devant les tribunaux.

3.3. Respect du droit à l'image

L'Utilisateur qui met à disposition ou qui exploite un support de communication mettant en situation l'image d'un collaborateur ou d'un tiers doit s'assurer préalablement du respect des dispositions légales en matière de droit à l'image et de respect de la vie privée.
Pour cela, il se rapprochera directement de la personne concernée pour recueillir son consentement préalable à l'utilisation de son image. Ledit consentement devra être consigné par l'Utilisateur par écrit et autoriser expressément l'étendue des droits d'utilisation

3.4. Respect de la loi « Informatiques & Libertés »

L'Utilisateur est informé de la nécessité de respecter les dispositions légales et/ou réglementaires en matière de traitement automatisé de données à caractère personnel (4), conformément à la loi « Informatique et Libertés » et au Règlement Général sur la Protection des Données (RGPD). En conséquence, si dans l'accomplissement de sa mission, l'Utilisateur est amené à procéder à un tel traitement, il devra s'assurer que les obligations légales et/ou réglementaires en matière de loi « Informatique et Libertés » sont respectées. Pour cela, il se rapprochera de la Direction Métier responsable de ce traitement dans l'Entreprise (5), afin qu'elle puisse, en collaboration avec les Services Juridiques et le Délégué à la Protection des Données, fixer les règles de gestion et les niveaux de protections adéquats à la mise en conformité. Cela permettra également de réaliser les démarches nécessaires auprès de la Commission Nationale Informatique & Libertés (CNIL) et en recevoir l'autorisation le cas échéant. En outre, toute opération réalisée lors d'un traitement de données à caractère personnel devra respecter la finalité de ce traitement, la pertinence des données collectées/traitées, les droits des personnes concernées, les durées maximales de conservation ainsi que la sécurisation de ces données.

(4) Tel que défini dans le préambule
(5) Par exemple, la Direction Marketing pour un traitement relatif aux données clients

Par ailleurs, conformément aux dispositions de ces textes, chaque Utilisateur dispose d'un droit d'accès, d'information, de rectification et d'opposition pour motif légitime relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des Systèmes d'Information. Conformément à la loi 2016-1321 du 7 octobre 2016, dite "Loi pour une République Numérique", chaque Utilisateur dispose du droit de définir des directives relatives au sort de ses données à caractère personnel après sa mort. Ces droits s'exercent auprès du responsable métier du traitement.

3.5. Respect de l'intégrité et de la disponibilité du Système d'Information

L'Utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement du Système d'Information de l'Entreprise, que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels malicieux connus sous le nom générique de virus, chevaux de Troie, bombes logiques, vers, etc.

L'implantation, l'utilisation, le développement ou la diffusion de programmes mettant en cause l'intégrité du Système d'Information sont interdits.

Il est interdit de se livrer, depuis des Ressources appartenant au Système d'Information de l'Entreprise, à des actes mettant sciemment en péril la sécurité ou le bon fonctionnement de Systèmes d'Information externes.

Le simple fait d'accéder à un système sans autorisation constitue un délit, même s'il n'en résulte aucune altération des données ou du fonctionnement dudit système.

3.6. Respect de la Confidentialité

L'accès par les Utilisateurs aux informations conservées sur le Système d'Information de l'Entreprise doit être limité à celles qui leur sont propres, et celles qui sont publiques ou partagées.
En particulier, il est interdit de prendre connaissance ou copier des informations détenues par d'autres Utilisateurs sans leur consentement, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations et correspondances privées de type courrier électronique dont l'Utilisateur n'est destinataire ni directement, ni en copie.
En toute hypothèse, l'Utilisateur doit agir conformément aux règles de classification des informations et de gestion des connaissances

3.7. Responsabilité en matière de transmission d'information

Les Ressources mises à disposition des Utilisateurs permettent l'accès à une communication et à une information importante et mutualisée. Or, de tels moyens ne doivent pas permettre de véhiculer n'importe quelle information. Il est notamment interdit, en toutes circonstances, de se livrer aux activités suivantes :

diffuser des messages diffamatoires ou injurieux, de harcèlement ou de menace ;
utiliser certaines formes d'apologie (crime, racisme, négationnisme) ;
collecter, stocker, consulter, publier, diffuser ou transmettre des messages et des œuvres à caractère violent, pornographiques, ou de nature à porter atteinte à la dignité humaine ;
utiliser toute forme de provocation à la haine raciale.

Ces activités sont illicites, quel que soit leur mode de diffusion, public ou privé. L'Utilisateur engage sa responsabilité civile et/ou pénale en cas de tels agissements.

En toutes circonstances, l'Utilisateur doit faire preuve de discernement et de prudence lorsqu'il échange des informations avec des tiers.

3.8. Contribution à l'amélioration du fonctionnement

Chaque Utilisateur doit contribuer à l'amélioration du fonctionnement du Système d'Information de l'Entreprise et à la sécurité de ce dernier. Sa contribution passe par :

Le respect des règles de sécurité et des lois applicables ;

la préservation de l'image de marque de l'Entreprise vis-à-vis de l'extérieur ;

Un signalement dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie de sécurité découverte (comme par exemple une tentative d'accès frauduleux aux Ressources et données dont il a la responsabilité) auprès de sa hiérarchie et/ou du correspondant sécurité de rattachement.

ARTICLE 4 : CONDITIONS SPÉCIFIQUES D'UTILISATION DES RESSOURCES

4.1. Messagerie professionnelle (messages électroniques et instantanées)

Les messageries électroniques et instantanées sont des outils professionnels, mis à la disposition de l'Utilisateur par l'Entreprise dans le cadre de l'exercice de sa mission, que ce soit via le système de messagerie électronique de l'Entreprise ou via la Plateforme.

Il est rappelé que les messages électroniques envoyés depuis un site de l'Entreprise vers un autre site de l'Entreprise ou du Groupe sont considérés comme sécurisés. Dans tous les autres cas, les messages transitent par l'Internet. Ils peuvent donc, à tout moment, être interceptés, visualisés, enregistrés et utilisés à d'autres fins par un tiers. L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un message manuscrit et peut être rapidement communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter des dysfonctionnements du Système d'Information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'Entreprise et/ou de l'utilisateur.
Il est par conséquent interdit d'utiliser des systèmes de messagerie publics sur l'Internet à des fins professionnelles relatives à l'activité de l'Entreprise.
Bien que la messagerie Internet ne garantisse ni la confidentialité des données, ni l'authenticité des messages provenant de l'extérieur de l'Entreprise, il est possible d'utiliser des outils de chiffrement répondant à ces besoins. Pour cela, l'Utilisateur doit en faire la demande auprès de son responsable informatique local.

En toute hypothèse, les échanges d'informations professionnelles doivent impérativement circuler par le système de messagerie électronique de l'Entreprise et/ou les systèmes de communication mis à disposition sur la Plateforme, de sorte que le renvoi automatique de messages professionnels vers un compte de messagerie personnel est notamment interdit.

4.1.1 Adresses électroniques

L'adresse de messagerie électronique attribuée par l'Entreprise doit être diffusée uniquement dans un but professionnel lié aux activités de l'Entreprise. Elle ne doit pas être diffusée afin de recevoir des messages sans rapport professionnel ou personnel, sauf nécessités de la vie courante. Un usage personnel modéré et raisonnable de l'adresse de messagerie électronique attribuée par l'Entreprise est toléré.

En effet, la divulgation non maîtrisée d'une adresse de messagerie augmente considérablement le risque d'apparition de courriers non sollicités (appelés « pourriels » ou « spams »).

4.1.2 Contenu des messages professionnels (électroniques et instantanés)

Un message électronique est un support écrit. Il doit avoir une forme et un contenu approprié à un mode de communication établi par l'Entreprise. De même que partout ailleurs, la courtoisie constitue une règle de base dans tous les échanges électroniques. L'Utilisateur est en conséquence responsable de la forme et du contenu des messages électroniques qu'il échange, au même titre que pour le courrier traditionnel.

Afin d'harmoniser les communications de l'Entreprise, les messages électroniques professionnels doivent comporter le nom et les coordonnées de l'auteur dudit message.
Toute mention complémentaire figurant au pied de page du courrier électronique doit être exactement conforme à la définition du poste occupé et respecter, le cas échéant, la charte graphique établie par les services compétents de l'Entreprise. L'Utilisateur doit ainsi s'abstenir de tenir tout propos dénigrant ou de nature à discréditer l'Entreprise, ses produits ou services, ses collaborateurs ainsi que ses partenaires (fournisseurs, clients, etc.).
Afin d'éviter toute ambiguïté dans la reconnaissance d'un courrier, l'Utilisateur doit explicitement identifier ce dernier au regard de son objet réel, en utilisant le champ « objet » du courrier électronique. Il est notamment interdit d'indiquer comme personnel des messages de nature professionnelle.

Il est possible d'attacher à un message électronique un ou plusieurs fichiers. Cependant, le système de messagerie n'est pas conçu pour transporter des fichiers volumineux. Par conséquent, la taille des fichiers attachés à un message (« pièces jointes ») est limitée techniquement par un mécanisme de quotas. L'Utilisateur doit veiller à respecter ce principe et utiliser des moyens d'échanges plus appropriés proposé par l'Entreprise lorsqu'il doit échanger des gros fichiers (serveurs de partage, serveurs d'échanges de fichiers, etc.).

L'utilisateur doit faire preuve de vigilance à l'égard des messages qu'il reçoit. A ce titre :

- Il n'ouvre pas les messages dont l'origine, l'objet ou le contenu est douteux. En cas de réception d'un tel message, il se conforme à l'information reçue par son service informatique et utilise les fonctionnalités de signalement prévues par l'outil (spam, phishing...)
- Il n'enregistre pas et n'exécute pas les pièces jointes suspectes.
- Il ne prend pas de décision importante à la seule vue d'un message électronique. En cas de doute, il contacte l'émetteur du message pour s'assurer de l'authenticité et de la véracité des informations reçues

4.1.3 Emission et réception de messages professionnels

L'Utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires réellement concernés, afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie, ainsi qu'une dégradation du service.

Il est strictement interdit de propager des messages collectifs, qui ne visent pas l'accomplissement d'une mission de travail, quel qu'en soit leur contenu, sauf autorisation expresse écrite et préalable de l'Entreprise.

4.1.4 Stockage et archivage des messages

Chaque Utilisateur est responsable de l'organisation et de la mise en œuvre des moyens nécessaires à la conservation de ses messages électroniques. L'Entreprise lui propose pour cela différents moyens de stockages, de sauvegarde et d'archivage.

4.1.5 Outils de contrôle

Pour assurer la sécurité de la messagerie électronique, l'Entreprise met en place de mécanismes automatiques de filtrage liés aux caractéristiques des messages électroniques : contenu, type de pièces jointes, taille, destinataires, etc.
Un logiciel anti-virus est également couplé avec le système de messagerie afin d'analyser systématiquement le contenu des pièces jointes dans les messages entrants. En cas de reconnaissance d'un logiciel malicieux dans une pièce jointe, celle-ci est détruite et les destinataires en sont informés. Cependant, il est possible qu'un message soit bloqué exceptionnellement par les outils automatiques de filtrage bien qu'il soit légitime. Il existe dans ce cas des procédures de récupération qui pourront être activées sur demande par l'Administrateur de la messagerie.

4.2. Internet / Intranet / Plateforme

L'accès à l'Internet est attribué individuellement à l'Utilisateur, afin de lui permettre de visiter, à des fins professionnelles, des sites du monde entier sous le nom de l'Entreprise. Cet accès peut être retiré à tout moment s'il en va de l'intérêt de l'Entreprise.

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle. Cependant, une consultation ponctuelle, et dans des limites raisonnables, de sites Internet, pour un motif personnel, est tolérée pourvu que les règles de sécurité ainsi que les principes
visés dans le présent document soient respectés.

4.2.1 Anonymat & préservation de l'image de marque

Toutes les activités de l'Utilisateur naviguant sur l'Internet, ainsi que les données concernant ce dernier (sites consultés, messages échangés, données fournies à travers de formulaires, données techniques de connexion, etc.) peuvent potentiellement être enregistrées à son insu par des tiers, puis analysées pour en déduire ses centres d'intérêt en vue d'une utilisation à des fins commerciales ou autres. Toutes les précautions doivent par conséquent être prises par l'Utilisateur à cet égard afin de préserver l'image de marque de l'Entreprise.

4.2.2 Téléchargements

Tout téléchargement de fichiers, notamment de sons, d'images ou de vidéos, sur le réseau Internet doit s'effectuer dans le respect du droit de propriété intellectuelle, tel que défini à l'article 3.2.
Si la visualisation d'un document téléchargé nécessite l'emploi d'un logiciel spécifique non disponible sur le poste de travail de l'Utilisateur, il convient de s'adresser au support bureautique de l'Entreprise pour obtenir les logiciels en question.

4.2.3 Forums, blogs, réseaux sociaux, communautés de la Plateforme

La participation de l'Utilisateur, pendant son temps de travail, à des espaces de discussion et des médias sociaux ouverts sur l'Internet est conditionnée par le respect des mêmes règles de courtoisie que la messagerie électronique sur les contenus publiés et ne peut intervenir, s'il s'agit d'une utilisation non professionnelle, que sous réserve d'une participation ponctuelle et modérée.

Il est interdit à l'Utilisateur d'exprimer sur les médias sociaux externes des opinions, des avis au nom et pour le compte de l'Entreprise, ni de se présenter comme un de ses représentants officiels, sans être directement autorisé par sa hiérarchie à remplir ce rôle. Les publications professionnelles sont, en effet, encadrées par une stratégie de communication définie par les directions mandatées de l'Entreprise.

La création par tout Utilisateur d'espaces de discussion et/ou de comptes sur des médias sociaux ouverts sur l'Internet, portant le nom commercial, la marque et/ou l'enseigne de l'Entreprise, et la participation de tout Utilisateur auxdits espaces et comptes, est conditionnée par le respect des mêmes règles de courtoisie que la messagerie électronique sur les contenus publiés et ne peut intervenir qu'après obtention d'une autorisation de l'Entreprise. Tous propos et contenus publiés par un Utilisateur sur ces espaces ou comptes étant susceptible d'engager la responsabilité de l'Entreprise, l'Utilisateur doit donc être particulièrement vigilant sur la teneur desdits propos et contenus publiés.

Les forums de discussion et blogs internes, disponibles sur l'Intranet de l'Entreprise, sont modérés. Sur les forums thématiques, il est de bon usage de respecter le cadre du thème fixé par les auteurs. Le modérateur de ces forums et blogs se réserve donc le droit de supprimer toute contribution qui contreviendrait à ces règles. En publiant sur ces espaces de communication, l'Utilisateur s'engage à respecter ces principes.
La liste des forums, blogs et de leurs modérateurs, ainsi que les éventuels guides pratiques de création d'espace et d'utilisation, sont disponibles sur l'Intranet de l'Entreprise. Les modalités de participation

aux communautés de la Plateforme sont disponibles sur la Plateforme et l'Utilisateur s'engage à en respecter les conditions générales d'utilisation.

En tout état de cause, tout propos et contenus publiés par un Utilisateur sur des forums, blogs, réseaux sociaux et/ou communautés de la Plateforme ne doit pas être contraire à la loi ni porter atteinte à l'image et à la réputation de l'Entreprise, de ses collaborateurs, de ses produits ou de ses partenaires (fournisseurs, clients, etc.).

L'Entreprise souhaite également alerter l'Utilisateur sur la nature et la portée des données personnelles qu'il communique et diffuse volontairement sur les forums, blogs, réseaux sociaux, et/ou communautés de la Plateforme. En effet, certains contenus sont susceptibles de fournir des informations à caractère sensible qui ne sont pas nécessaires à l'utilisation des différents services. Dans de telles hypothèses, il est rappelé à l'Utilisateur qu'il est le seul et unique responsable des informations qu'il fournit.

4.2.4 Outils et mesures de contrôle

Dans les limites prévues par la loi, l'Entreprise met en place un système de journalisation des accès Internet. Des outils assurant la traçabilité des actions (6) sont par conséquent mis en place sur le Système d'Information.

(6) Conservation des données techniques de connexion telles que la date et l'heure d'accès, l'adresse IP de l'utilisateur, l'identifiant utilisateur, l'URL accédée, la durée de connexion, etc.

Les données de connexion de l'Utilisateur sont enregistrées par l'Entreprise qui, à des fins de statistiques, de qualité de service et de sécurité, supervise le trafic Internet et effectue des audits réguliers du Système d'Information. La finalité de ces fichiers de journalisation est de contrôler et garantir une utilisation normale et non excessive des Ressources du Système d'Information.
L'Entreprise met également en place des mécanismes automatiques de filtrage liés à la catégorisation des sites Internet visités ou à des mots clés, conformément aux règles de droit applicables.
Dans le cas d'une violation manifeste de la politique de sécurité, les informations de journalisation concernant chaque Utilisateur pourront être utilisées comme éléments de preuve.

L'Utilisateur est informé que l'Entreprise est tenue de conserver ses données d'identification et de connexion à la Plateforme, conformément à la loi n°2004-575 du 21 juin 2004 dite « *Loi pour la confiance dans l'économie numérique* ».

La durée de rétention maximale des journaux d'audit est fixée à un an.

4.3. Nomadisme & Mobilité

L'Utilisateur de terminaux mobiles (téléphones intelligents, tablettes numériques & ordinateurs portables) est particulièrement vulnérable lorsqu'il se trouve en situation nomade à l'extérieur de l'Entreprise. Il doit par conséquent redoubler de vigilance dans la protection de ses équipements mobiles professionnels, afin de limiter les risques de perte ou de vol notamment.

L'Utilisateur s'engage à respecter les règles propres au nomadisme et à la mobilité de l'Entreprise. Des compléments d'information liés à cet usage sont disponibles dans les guides pratiques d'utilisation sur l'Intranet de l'Entreprise, ainsi que sur la Plateforme.

Une attestation de remise des terminaux mobiles professionnels délivrés à l'Utilisateur est signée en deux exemplaires par l'Entreprise et l'Utilisateur concerné. En toutes hypothèses, l'Entreprise reste et demeure l'unique propriétaire desdits terminaux mobiles professionnels.
Dans le cas particulier où l'Entreprise autorise les Utilisateurs à accéder aux Ressources du Système d'Information au moyen de terminaux mobiles personnels, cet usage est encadré par une politique de sécurité spécifique, disponible sur l'Intranet de l'Entreprise et sur la Plateforme.

ARTICLE 5 : MESURES CONSERVATOIRES

L'Entreprise se réserve le droit de limiter ou suspendre les usages du Système d'Information par mesure conservatoire. Cette décision peut intervenir en cas de suspension du contrat de travail ou de l'activité de l'Utilisateur, pour quelque motif ou quelque cause que ce soit, de défaillance technique, d'utilisation inappropriée, volontaire ou involontaire, ainsi qu'en cas de force majeure menaçant la continuité d'activité de l'Entreprise.

Sous condition d'autorisation du directeur ou du responsable du service concerné, l'Administrateur pourra ainsi, après avoir informé le Correspondant Sécurité :

suspendre ou retirer des droits d'accès de l'Utilisateur, avec information de celui-ci sauf impossibilité ou circonstances particulières, à tout ou partie du Système d'Information ;

effacer, isoler ou neutraliser toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des Systèmes d'Information.

ARTICLE 6 : SANCTIONS

En cas de violation avérée de la présente Charte, Auchan pourra prendre des sanctions disciplinaires adaptées à la gravité des agissements conformément aux dispositions du règlement intérieur.

En cas de non-respect de la législation en vigueur, l'Utilisateur sera tenu responsable de ses actes et pourra encourir des sanctions légales (civiles ou pénales) prévues par la loi.

ARTICLE 7 : INFORMATION & FORMATION DES COLLABORATEURS

La présente Charte est portée à la connaissance de chaque Utilisateur par toute voie jugée nécessaire par l'Entreprise et sous toute forme de communication utile, conformément à l'article R. 1321-1 du Code du travail.

Elle est disponible sur l'Intranet de l'Entreprise, ainsi que des guides pratiques associés. Elle est par ailleurs insérée dans le dossier d'accueil des nouveaux collaborateurs
Dans l'éventualité où l'Utilisateur aurait des questions ou ne comprendrait pas certaines des règles et prescriptions de sécurité prévues par la présente charte il peut contacter par écrit et à tout moment son Correspondant sécurité.

Des opérations de communications internes sont organisées régulièrement, afin d'informer les Utilisateurs sur l'évolution des pratiques d'utilisation des NTIC recommandées par l'Entreprise.
Une formation spécifiquement adaptée accompagne l'évolution des missions des collaborateurs qui le requièrent.

ARTICLE 8 : ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte est applicable à compter de l'entrée en vigueur du règlement intérieur. Elle a été adoptée après information et consultation des instances représentatives du personnel de l'Entreprise

Annexe 3

Code de conduite

- Le présent code de conduite a pour objectif de traduire certaines dispositions de la loi Sapin 2, imposant aux grandes entreprises de mettre en place un dispositif de prévention en matière de corruption et trafic d'influence.

  Le code de conduite doit « *définir et illustrer les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou trafic d'influence* ». (article 17 II de la loi Sapin 2). Selon ces dispositions légales, ce code doit être intégré au règlement intérieur.

- Ce code est applicable à l'ensemble des collaborateurs, et précise les comportements à risque dans les relations entre les collaborateurs et vis-à-vis d'intermédiaires ou fournisseurs agissant pour le compte de l'entreprise.

  Toute infraction à ce code peut avoir des conséquences juridiques et financières graves, mais aussi nuire durablement à la réputation de l'entreprise. Il est donc essentiel de respecter ces recommandations.

- Toute violation grave du présent code pourrait donner lieu à l'application de l'une des sanction prévue par le règlement intérieur.

- **Définitions**

La corruption est le fait de solliciter ou d'accepter des cadeaux, des avantages, des dons pour accomplir un acte résultant de ses fonctions ou avoir accepter de faciliter un acte en échange de cadeaux, avantages, dons.

Le trafic d'influence est commis par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public afin de solliciter des avantages ou d'abuser de son influence.

Seule la corruption sera donc abordée dans cette annexe.

Ainsi tout collaborateur doit refuser tout cadeau personnel, invitation, don, avantage, ou facilité, d'une valeur déraisonnable et de façon non occasionnelle de la part d'un autre collaborateur, client, fournisseur, prestataire, dans le but d'obtenir un avantage ou une décision, d'influencer une position.

Un collaborateur s'interdit de proposer de tels cadeaux ou avantages dans le but d'obtenir une décision ou d'influencer une position d'un autre collaborateur, client, prestataire, fournisseur.

Dans le cas où un collaborateur est destinataire d'un cadeau ou invitation dans le contexte décrit ci-dessus il s'engage à le retourner à l'entreprise et à en faire part à son supérieur hiérarchique.

Le collaborateur est en droit d'accepter un cadeau ou geste habituel ou usuel dans les relations professionnelles concernées, de valeur symbolique. Dans ce cas, il n'en fait pas un usage personnel mais le partage dans la mesure du possible avec ses collègues de travail.

En cas de doute sur le caractère habituel ou usuel du cadeau, ou sa valeur symbolique, le collaborateur en fait part préalablement à son supérieur hiérarchique.

La valeur symbolique d'un cadeau peut s'apprécier par comparaison avec la valeur d'un cadeau qui serait réalisé dans la vie personnelle, dans un cercle familial ou amical.

De même, un collaborateur doit s'abstenir de monnayer l'influence d'une personne dans le but de favoriser la décision qui serait prise par un tiers, même si cette décision favorise l'intérêt exclusif de l'entreprise.

En cas de doute le collaborateur doit impérativement consulter préalablement son responsable des ressources humaines, ou son supérieur hiérarchique.

- **Exemples de comportements susceptibles de caractériser un fait de corruption :**

  - Face à une urgence, un manager discute avec son contrôleur de gestion sur la possibilité de s'assurer des services d'une agence de travail temporaire que sa belle-sœur dirige. Son collègue lui répond que cela pose un problème du fait de son lien personnel avec une personne de cette

agence et qu'il est indispensable d'en parler clairement à son supérieur avant toute démarche d'appel d'offre ou de référencement.

- Dans le cadre d'une relation avec un prestataire, celui-ci a une phrase du type « on sait remercier les personnes qui nous aident à développer notre affaire... » le collaborateur indique à son interlocuteur que notre entreprise ne partage pas ces pratiques et qu'il sera contraint de faire cesser leurs relations professionnelles si ce type de sollicitations perdurent.

- Un collaborateur se voit proposer une invitation une fois par mois dans un restaurant gastronomique réputé de la part d'un prestataire afin que soit préservé l'exclusivité de leur relation. Il doit être interpellé par la fréquence de ces invitations, les refuser et en faire part à son supérieur hiérarchique.

- Un collaborateur se voit demander par un employé d'un prestataire une somme d'argent afin d'obtenir une livraison plus rapide de produits attendus en urgence. Il demande à quoi cette somme d'argent correspond. En l'absence de vraie réponse, il demande une confirmation écrite du supérieur de l'employé et une facture.

- Deux responsables discutent d'un projet d'ouverture d'un entrepôt dans une nouvelle région, l'un des deux dit : « il va falloir approcher les autorités régionales que nous ne connaissons pas. L'un des deux lui rappelle que notre entreprise ne pratique pas les « petites attentions » et que nous devons être particulièrement vigilants sur la qualité du dossier.

- Un responsable reçoit dans son bureau une entreprise du bâtiment qui doit travailler en magasin et demande d'effectuer, en échange du marché, des travaux personnels à son domicile. Ce comportement est contraire aux valeurs éthiques, car l'intérêt personnel ne peut primer sur l'intérêt de l'entreprise.