CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES

Carrefour Banque

Annexe au règlement intérieur

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

Objet du document

Ce document décrit l'annexe au Règlement Intérieur : la Charte d'Utilisation des Ressources Informatiques.

Cette charte est à destination des salariés travaillant pour le compte de la société Carrefour Banque. Elle est annexée au règlement intérieur conformément au chapitre VII de ce dernier.

Tableau de Validation

Rédaction	Vérification	Approbation
Carrefour Banque(Service Juridique, RH, SSI)	Conformité	Comité SSI, Ressources Humaines

Révisions

Version	Date	Modification(s)
2.0	Aout 2013	Modifications de la Charte par le GIE CPFS
1.0	2013	Charte SI Carrefour France
3.1	2021	Charte SI Carrefour Banque

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

Table des matières

Objet du document 2
Tableau de Validation 2
Révisions 2
Table des matières 3
PREAMBULE 4
ARTICLE 1 : CHAMP D'APPLICATION ET STATUT DE LA CHARTE 5
ARTICLE 2 : REGLES GENERALES RELATIVES A LA PROTECTION DES RESSOURCES INFORMATIQUES 6
Article 2.1. : Protection de l'identité de l'Utilisateur et de l'accès aux Ressources Informatiques 6
Article 2.2 : Protection de l'intégrité du poste de travail (poste fixe, équipement nomade ou tout autre terminal) 6
Article 2.3 : La protection spécifique des équipements nomades 7
Article 2.4 : Protection contre une utilisation des Ressources Informatiques à des fins illicites 8
a. Protection des droits de la personne 8
b. Protection de la propriété industrielle et intellectuelle des tiers 8
c. Protection des droits industriels et intellectuels du Groupe 9
d. Protection de l'image de marque, de la réputation, des ressources et des biens du Groupe 9
ARTICLE 3 : REGLES RELATIVES A L'UTILISATION DES MATERIELS, PROGRAMMES, LOGICIELS ET FICHIERS ET A L'ACCES AUX INFORMATIONS ET DONNEES 10
Article 3.1 : Utilisation des matériels, programmes, logiciels et fichiers 10
Article 3.2 : Accès aux informations et données 10
ARTICLE 4 : ACCES A INTERNET 11
ARTICLE 5 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE ET DES TRANSFERTS DE FICHIERS 12
ARTICLE 6 : UTILISATION DES RESSOURCES INFORMATIQUES A DES FINS EXTRA-PROFESSIONNELLES, NOTAMMENT UTILISATION A DES FINS PRIVEES, PARTICIPATION A DES RESEAUX SOCIAUX 13
Article 6.1 : Utilisation des Ressources Informatiques à des fins extra-professionnelles, notamment utilisation à des fins privées 13
a. Utilisation de la messagerie électronique 13
b. Usage d'internet 14
c. Stockage de données 14
d. Absences, départ de l'Entreprise, autres cas particuliers 14
Article 6.2 : Réseaux sociaux, forums de discussion externes 15
ARTICLE 7 : VIGILANCE DE CHAQUE UTILISATEUR 17
ARTICLE 8 : MOYENS DE CONTROLE ET AUDITS 17
ARTICLE 9 : SANCTIONS 18
ANNEXES 20
Annexe 1 : Règle de Classification des Données 20

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

PREAMBULE

La société Carrefour Banque, (ci-après la « **Société** » ou l'« **Entreprise** ») est une filiale de Carrefour (60%) et de BNPP PF (40%) depuis 1985 et fait partie du Groupe Carrefour, ci-après le « Groupe ».

La Société est ainsi amenée à mettre à la disposition de ses utilisateurs des « **Ressources Informatiques** » qui sont constituées par :

- les informations et les données susceptibles d'être stockées (exemples : bases de données, images) et qui circulent notamment :
  - entre les utilisateurs ;
  - entre les utilisateurs et l'externe (personnes travaillant pour une autre entité du Groupe ou pour une entreprise n'appartenant pas au Groupe) ;

- les équipements des technologies de l'information tels que back office, de radiofréquence, etc. ;

- les infrastructures de réseaux et de télécommunications ;

- les applications et les logiciels standards ou spécifiques, les bases de données, les sites intranet, etc. ;

- le matériel bureautique (ordinateurs, imprimantes, appareils et périphériques nomades etc.) ;

Les Ressources Informatiques sont la propriété du Groupe ou sont mises à la disposition des Utilisateurs. Il est ici rappelé que tout matériel obsolète ou qui n'est plus utilisable pour tout motif reste la propriété du Groupe et est soumis aux procédures de déclassement.

Le Groupe décide de la finalité, de l'attribution et de l'utilisation de ces ressources mises à disposition des utilisateurs à des fins professionnelles.

La Société est par ailleurs susceptible de fournir aux utilisateurs les services informatiques au sens large (maintenance, support, prestations diverses, développement de programme etc.).

Est considéré comme « **Utilisateur** », toute personne, quel que soit son statut (salarié, personnel de travail temporaire, stagiaire, personnel mis à disposition, intervenant extérieur, mandataires sociaux etc.) qui est amenée à accéder aux Ressources Informatiques ou, à créer, modifier, consulter, manipuler et plus généralement utiliser des Ressources Informatiques.

Il est rappelé que certains Utilisateurs sont :

- **des gestionnaires des systèmes d'information** faisant partie des Ressources Informatiques ayant une habilitation de niveau « administrateur ». Ils sont amenés, dans le cadre de leurs fonctions de surveillance et de contrôle du fonctionnement du Système d'Information, à avoir accès à des informations relatives aux autres Utilisateurs.

  Par ailleurs, ces administrateurs sont amenés à utiliser des logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou prendre le contrôle à distance du poste de l'Utilisateur, sous réserve de l'accord préalable de l'Utilisateur.

  Ces interventions conformes aux dispositions légales et réglementaires en vigueur ne sont réalisées que si elles sont nécessaires pour assurer le bon fonctionnement et la sécurité des Systèmes d'Information ou à des fins de contrôles conformément à l'article 8 de la présente charte.

  Ces gestionnaires des systèmes d'information sont soumis une obligation de confidentialité et ne doivent pas divulguer d'informations considérées comme confidentielles qu'ils peuvent être amenés à connaître dans le cadre de l'exercice de leurs fonctions sauf si celles-ci portent atteinte au bon fonctionnement des systèmes d'information et à leur sécurité ou conformément aux dispositions de

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

l'article 8 de la présente charte, et ce sous réserve du respect des dispositions légales, réglementaires et jurisprudentielles applicables en la matière.

- **des chefs de projet**. Ces derniers sont amenés, dans le cadre de leurs fonctions, à piloter des projets relatifs aux systèmes d'information visant la mise en place ou la modification de Ressources Informatiques ou de processus fonctionnels. Les chefs de projet devront s'assurer qu'une analyse de risques a été menée conformément aux standards en vigueur dans l'Entreprise et cela dès les premières phases d'un projet. Les chefs de projet pourront s'adresser, en cas de besoin, au Responsable de la Sécurité des Systèmes d'Information de la Société afin de réaliser ou de faire réaliser cette analyse de risque.

Les Ressources Informatiques sont mises à la disposition des Utilisateurs à des fins essentiellement professionnelles, tournées vers la performance de la Société et du Groupe et la satisfaction de ses clients. De ce fait, il incombe à tout Utilisateur de veiller à protéger :

- les Ressources Informatiques, notamment les équipements, les systèmes et les données contre la perte, la destruction, les atteintes à l'intégrité, la falsification des sources, la perturbation du fonctionnement, l'augmentation indue des coûts de fonctionnement, et tout autre acte ou événement illicite et/ou susceptible de porter atteinte aux intérêts de la Société ou du Groupe.

- les accès aux Ressources Informatiques contre notamment les atteintes à la confidentialité des données et des traitements, la violation des droits des tiers, les détournements à des fins personnelles non autorisées, l'usurpation ou le masquage d'identité, et plus généralement l'utilisation à des fins illicites et/ou susceptible de porter atteinte aux intérêts de la Société ou du Groupe.

Chaque Utilisateur doit être conscient que, d'une part, l'usage de Ressources Informatiques obéit à des règles, notamment celles objet de la présente charte, qui s'inscrivent dans le respect de la loi, de la sécurité et de l'intérêt de la Société et/ou du Groupe et que, d'autre part, la négligence ou la mauvaise utilisation de ces ressources peut faire courir des risques parfois très significatifs à la Société, au Groupe, voire à des Utilisateurs individuellement.

Ainsi, chaque Utilisateur doit appliquer l'ensemble des dispositions relatives à l'utilisation des Ressources Informatiques de la présente charte, que cela soit à l'intérieur ou à l'extérieur des locaux de l'Entreprise.

ARTICLE 1 : CHAMP D'APPLICATION ET STATUT DE LA CHARTE

La présente charte a pour vocation :

- de formaliser au sein de l'Entreprise les règles générales de déontologie et de sécurité relatives à l'utilisation des Ressources Informatiques,
- de préciser la responsabilité des Utilisateurs des Ressources Informatiques.

Chaque Utilisateur doit appliquer l'ensemble des dispositions de la présente charte.

Si l'Utilisateur éprouve une difficulté à mettre en œuvre l'une des dispositions de la présente charte, il doit en référer immédiatement à sa hiérarchie et/ou au Responsable de la Sécurité des Systèmes d'Information de la Société.

La présente charte qui annule et remplace la charte actuellement en vigueur au sein de la Société constitue une annexe du règlement intérieur et entre en vigueur le xx/xx/2021.

Il est fait référence à la définition du champ d'application et aux dispositions relatives aux procédures et sanctions disciplinaires, si applicables, du règlement intérieur de la Société.

En complément de cette charte, la Société a mis et continuera à mettre en place des moyens, en particulier informatiques, des procédures et des recommandations pour l'utilisation des Ressources Informatiques.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

ARTICLE 2 : REGLES GENERALES RELATIVES A LA PROTECTION DES RESSOURCES INFORMATIQUES

Article 2.1. : Protection de l'identité de l'Utilisateur et de l'accès aux Ressources Informatiques

L'identifiant (couple login/mot de passe) est personnel et ne doit être communiqué à quiconque.

Sa composition et son unicité sont définies et contrôlées par les gestionnaires du système d'information selon des principes établis par l'Entreprise. Cette règle de sécurité interdit les identifiants « génériques » car ils sont contraires au principe d'imputabilité des actions et aux règles d'audit. Elle s'applique non seulement à tous les collaborateurs de l'entreprise mais aussi à toute personne dûment autorisée à accéder aux systèmes, applications et données de l'entreprise.

En cas de perte ou de vol d'un élément identifiant, l'Utilisateur s'engage à informer immédiatement son supérieur hiérarchique ou le Responsable de la Sécurité des Systèmes d'Information de la Société.

Il est de la responsabilité de chaque Utilisateur de choisir un mot de passe qui soit conforme aux recommandations des gestionnaires des systèmes d'information de l'Entreprise. Ce mot de passe doit toujours être à minima alphanumérique, d'une longueur au moins égale à 8 caractères, être renouvelé régulièrement et ne pas être inscrit à proximité du poste de travail ni enregistré dans un fichier électronique que cela soit sur le poste de travail ou sur un périphérique nomade (téléphone, assistant personnel, etc.).

L'Entreprise pourra revoir régulièrement ces recommandations et les communiquer à l'Utilisateur par tout moyen et ce, en fonction des nouveaux impératifs en terme de sécurité des systèmes d'information.

La complexité des mots de passe étant un paramètre essentiel à la sécurisation des systèmes d'information, des audits de sécurité sur les mots de passe peuvent être réalisés par les services dûment habilités.

Dans le cadre de ces audits, des mots de passe, dont la complexité ne serait pas suffisante, peuvent ainsi être déchiffrés. Les résultats de ces audits sur les mots de passe ont pour unique finalité l'établissement de statistiques sur le niveau de sécurité des systèmes d'information et la détermination des éventuelles mesures qui seraient nécessaires, au niveau de l'entreprise, au renforcement de cette sécurité. En aucun cas, ils ne pourront être utilisés à d'autres fins.

L'usurpation d'identité est interdite quelle qu'en soit la finalité.

Lorsque l'Utilisateur quitte son poste de travail, même pour une courte durée, il doit le verrouiller afin de le rendre inaccessible.

L'accès aux Ressources Informatiques de tout poste de travail ou outil non configuré par les gestionnaires du système d'information du Groupe (notamment les ordinateurs portables) est soumise à une autorisation délivrée par le service dûment accrédité afin qu'une vérification du niveau de protection et de configuration du poste ou de l'outil soit réalisée.

Article 2.2 : Protection de l'intégrité du poste de travail (poste fixe, équipement nomade ou tout autre terminal)

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

Chaque Utilisateur doit veiller à conserver en l'état les dispositifs de sécurité installés sur son poste de travail, équipement nomade ou autre terminal (le « **Poste** ») :

- seuls les gestionnaires du système d'information dûment habilités peuvent modifier les paramètres des systèmes d'information.

- il est interdit de rendre inopérants et de limiter les dispositifs de sécurité mis en place, notamment en désactivant les anti-virus ou en ajoutant des matériels ou des logiciels externes aux systèmes d'information à l'exception des supports de stockages amovibles dans les conditions fixées aux articles 3 et 6 de la présente charte.

Seuls certains gestionnaires des systèmes d'information ont une habilitation de niveau « administrateur » leur permettant de réaliser des opérations spécifiques. Toutefois des dérogations exceptionnelles pourront être accordées à d'autres Utilisateurs si leur mission le justifie et ce, après validation du Directeur des Systèmes d'Information ou du Responsable de la Sécurité des Systèmes d'Information de la Société.

Il est ici rappelé que les composants des systèmes d'information et plus généralement les Ressources Informatiques ne peuvent être acquis, installés, attribués, modifiés, supprimés, faire l'objet d'un accès, d'un traitement ou de toute manœuvre manipulant leur fonctionnement, ou être utilisés que par des personnes dûment autorisées. En particulier, tout logiciel doit faire l'objet d'une validation, tant sur le plan technologique que sécurité, préalablement à sa mise à disposition et à son utilisation par un Utilisateur de l'Entreprise.

Il est également rappelé que toute installation de logiciel implique généralement le règlement par l'Entreprise d'une redevance d'utilisation versée aux éditeurs et est soumise à des conditions d'utilisation (« Conditions de Licence ») que l'Entreprise doit respecter et faire respecter par les Utilisateurs. Aussi, toute utilisation de logiciel dans l'entreprise qui ne respecterait pas les conditions de licence serait constitutive d'une violation de la législation en matière de Propriété Intellectuelle, laquelle peut donner lieu à des sanctions pénales et civiles. Il est donc rappelé aux Utilisateurs qu'il est interdit par la loi et notamment les dispositions du Code de la Propriété Intellectuelle d'installer un logiciel ne faisant pas l'objet d'une licence régulièrement acquise, de le copier en un nombre d'exemplaires supérieur à celui autorisé aux termes des conditions d'utilisation autorisées, de le modifier etc.

Dans le cas où l'Utilisateur aurait besoin d'un nouveau matériel et/ou logiciel ou de modifier ceux-ci, il devra en effectuer la demande auprès de sa hiérarchie ou des services compétents de l'Entreprise, seuls autorisés à modifier la configuration des Ressources Informatiques et/ou à mettre à sa disposition des moyens supplémentaires.

L'Utilisateur doit signaler dans les plus brefs délais au service support utilisateurs ou à tout autre service désigné à cet effet, les situations de fonctionnement de Ressources Informatiques mis à sa disposition qu'il jugera anormales, par exemple : détection ou suspicion d'un virus, perte de contrôle du poste de travail, etc.

L'Utilisateur s'interdit tout acte malveillant. Ainsi, il est strictement interdit de porter atteinte à l'intégrité et à la disponibilité des Ressources Informatiques, notamment en les perturbant volontairement, par exemple par des manipulations de nature à fausser ou entraver le bon fonctionnement desdites ressources, notamment par des actions de destruction physique ou logique ou par l'introduction de logiciels malicieux (ver, virus, bombe logique, etc.).

Article 2.3 : La protection spécifique des équipements nomades

Les équipements nomades (téléphone mobile professionnel, ordinateur portable, et plus généralement tout type de Ressources Informatiques portable ou amovible) constituent une extension du système d'information du Groupe et font ainsi partie intégrante des Ressources Informatiques. Ils sont susceptibles de transporter en dehors des locaux de l'Entreprise un certain nombre de données telles que les coordonnées de collaborateurs du Groupe et de fournisseurs, éventuellement une version électronique de l'agenda de son propriétaire, des photos, des fichiers divers etc.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

L'Utilisateur devra notamment prendre toutes les dispositions nécessaires visant à éviter le vol de ses équipements nomades (utilisation de cadenas, autres dispositifs autorisés de sécurité etc.) ou de ses données.

De plus, il est rappelé à l'Utilisateur que dans le cas de l'utilisation d'un réseau non administré par l'Entreprise ou le Groupe (réseau personnel, accès wifi, etc.), il doit toujours s'assurer que l'accès qu'il utilise se fait dans des conditions de sécurité suffisantes. Ainsi l'Utilisateur doit-il toujours veiller à ne pas utiliser un accès réseau non protégé.

Enfin, l'Utilisateur doit toujours veiller à respecter les dispositions de cette charte et ce, quel que soit l'endroit à partir duquel l'Utilisateur accède aux Ressources Informatiques via un équipement nomade.

Article 2.4 : Protection contre une utilisation des Ressources Informatiques à des fins illicites

a. Protection des droits de la personne

L'Utilisateur s'interdit d'utiliser les Ressources Informatiques à des fins de harcèlement, d'injures, de manière déloyale ou plus généralement à des fins illicites et/ou susceptible de porter atteinte aux intérêts de la Société ou du Groupe.

L'Utilisateur ne doit, en aucune circonstance, charger, stocker, publier, diffuser ou distribuer, au moyen des Ressources Informatiques, des documents, informations, images, vidéos et plus généralement des données :

- à caractère violent, pornographique ou contraire aux bonnes mœurs,
- susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
- à caractère injurieux ou diffamatoire,
- à caractère sexiste ou discriminatoire,
- à caractère raciste, négationniste ou xénophobe,
- susceptibles de porter atteinte à la vie privée des personnes,
- ou de manière générale interdits par la loi ou des règlements en vigueur et/ou sanctionnés pénalement.

Il est interdit d'accéder à des serveurs internet présentant ces caractéristiques. Si l'Utilisateur a reçu de tels éléments, il est tenu de le signaler immédiatement au Responsable de la Sécurité des Systèmes d'Information de la Société. Il est toutefois ici précisé qu'en cas d'atteinte à l'image de la Société ou du Groupe portée par ces sites, la consultation des données y étant relatives sera autorisée aux seules personnes devant assurer la protection des intérêts de la Société ou du Groupe.

b. Protection de la propriété industrielle et intellectuelle des tiers

L'Utilisateur s'interdit de :

- charger, stocker ou transmettre des fichiers ou plus généralement des données contenant des éléments protégés par le Code de la Propriété Intellectuelle, sauf à y être habilité au titre des licences ou autorisations nécessaires ;

- charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, œuvres multimédia, bases de données ou plus généralement des données qui sont protégés par le Code de la Propriété Intellectuelle, sauf à y être habilité au titre des licences ou autorisations nécessaires, ou de solliciter l'envoi par des tiers de tels fichiers, programmes, logiciels, progiciels ou données ;

- utiliser, de manière contraire aux règles du Code de la Propriété Intellectuelle, des règles techniques applicables et des prescriptions définies par la Société, les matériels, programmes, logiciels, progiciels

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

et autres outils mis à sa disposition par le Groupe ou auxquels il accéderait de quelque manière que ce soit ;

- utiliser, de reproduire, de détruire ou de modifier les codes sources ou le code exécutable de tout programme, logiciel ou progiciel mis à sa disposition par le Groupe ou auxquels il accéderait de quelque manière que ce soit, en violation du Code de la Propriété Intellectuelle, des règles techniques applicables et des prescriptions définies par la Société.

Les logiciels, progiciels et autres outils informatiques doivent être utilisés conformément aux conditions des licences souscrites par la Société ou le Groupe.

A cet égard, la Société met à disposition des Utilisateurs (par diffusion et publication sur un intranet) une « librairie des logiciels Carrefour Banque » qui a pour objectif de référencer les seuls logiciels qui sont autorisés à être installés par les gestionnaires du système d'information en accord avec le processus de déploiement des logiciels en vigueur dans l'Entreprise et le Groupe.

L'installation des logiciels peut être réalisée soit par une intervention individuelle (directement sur le Poste de l'Utilisateur par une personne expressément habilitée ou par télémaintenance) ou par un déploiement en télédistribution.

Dans l'objectif de la maîtrise de son parc logiciel et notamment de la bonne gestion de ses droits d'utilisation de ses logiciels, la Société a mis en place un outil informatique permettant de réaliser automatiquement des inventaires d'installation ou d'utilisation des logiciels, voire de procéder à des désinstallations automatiques de logiciels qui seraient ou non référencés dans la librairie des logiciels de l'Entreprise ou du Groupe.

c. Protection des droits industriels et intellectuels du Groupe

L'Utilisateur s'interdit de porter atteinte d'une quelconque manière, aux droits de propriété industrielle et intellectuelle de l'Entreprise ou du Groupe, portant notamment sur les œuvres multimédia, bases de données et sites internet/intranet de l'Entreprise ou du Groupe.

d. Protection de l'image de marque, de la réputation, des ressources et des biens du Groupe

L'Utilisateur ne doit jamais :

- charger, stocker, publier, diffuser ou distribuer des documents, informations, images, vidéos ou autres données portant atteinte à l'image de marque interne et externe et/ou à la réputation de la Société ou du Groupe. Cette restriction ne s'appliquera pas, en cas d'atteinte à l'image de la Société ou du Groupe, aux personnes devant assurer la protection des intérêts de l'Entreprise ou du Groupe.

- charger, stocker, publier, diffuser ou distribuer des documents, informations, images, vidéos ou autres données portant atteinte aux ressources et biens de l'Entreprise et plus particulièrement à l'intégrité, à la confidentialité et à la conservation de ses données ;

- charger, stocker ou transmettre, sciemment, des fichiers contenant des virus ou autres dispositifs malveillants ou des données altérées. Si l'Utilisateur reçoit de tels éléments, il est tenu de le signaler immédiatement au Responsable de la sécurité du système d'information de l'Entreprise ;

- exploiter les éventuelles failles de sécurité des Ressources Informatiques qu'il pourrait découvrir ou dont il pourrait avoir connaissance. Si l'Utilisateur apprend l'existence de telles failles de sécurité, il est tenu de le signaler immédiatement au Responsable de la Sécurité du Système d'Information de l'Entreprise ;

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

- porter atteinte, et plus particulièrement de faire obstacle et/ou contourner le dispositif permettant d'assurer la sécurité des Ressources Informatiques.

ARTICLE 3 : REGLES RELATIVES A L'UTILISATION DES MATERIELS, PROGRAMMES, LOGICIELS ET FICHIERS ET A L'ACCES AUX INFORMATIONS ET DONNEES

Article 3.1 : Utilisation des matériels, programmes, logiciels et fichiers

Le disque dur ou support de stockage de données du poste de travail et plus généralement des Ressources Informatiques mises à la disposition d'un Utilisateur ne doivent pas contenir de programmes, logiciels, documents, fichiers, informations ou données, tels que rappelés à l'article 2.4 de la présente charte, et notamment des logiciels, fichiers ou données à caractère pornographique, pédophile, raciste, négationniste, xénophobe, injurieux, sexiste, discriminatoire ou de manière générale, interdits par la loi ou des règlements en vigueur et/ou sanctionnés pénalement.

Il est rappelé que l'introduction d'équipements informatiques privés dans l'entreprise ou dans son Système d'Information n'est pas autorisée, sauf cas particulier soumis à un accord préalable de la Direction des Systèmes d'Information Carrefour Banque.

L'Utilisateur s'engage à préserver l'intégrité des systèmes informatiques et plus généralement des Ressources Informatiques et à ne pas apporter de perturbations aux systèmes par exemple par des manipulations de nature à fausser ou entraver le bon fonctionnement desdites ressources, notamment par des actions de destruction physique ou logique ou par l'introduction de logiciels malicieux (ver, virus, bombe logique, etc.).

Article 3.2 : Accès aux informations et données

L'Utilisateur est responsable des droits d'accès à ces documents, informations ou données (par exemple en lecture seule ou pour modification) qu'il peut donner à d'autres Utilisateurs.

Les Utilisateurs ayant accès à des informations et données comportant des données confidentielles et/ou à caractère personnel devront mettre en œuvre les procédures de l'Entreprise permettant d'assurer une protection appropriée pour l'utilisation de ces données et ce, notamment durant le stockage et le transfert de celles-ci et plus généralement veiller à ce que les restrictions d'accès et d'utilisation concernant notamment ces données confidentielles et/ou nominatives soient respectées.

Le niveau de protection évolue en fonction notamment du développement des techniques. Toute nouvelle disposition définie par l'Entreprise en matière de protection des données sera communiquée à l'Utilisateur par sa hiérarchie, le Responsable de la Sécurité des Systèmes d'Information de la Société ou tout autre moyen de communication adapté.

Afin que les restrictions d'accès et d'utilisation concernant notamment les données confidentielles telles que classées suivant la classification figurant en annexe de la présente charte et/ou à caractère personnel soient respectées, il est interdit à l'Utilisateur de consulter ou transmettre, modifier ou détruire ces données, sauf autorisation expresse accordée dans la cadre de ses missions, par toute personne habilitée.

L'Utilisateur s'interdit d'ouvrir et de prendre connaissance, de charger, d'intercepter, de détourner, d'utiliser, de stocker, de copier, de diffuser, de modifier ou de supprimer, toute donnée ou fichier informatique dont il n'est pas destinataire et auxquels il n'est pas censé avoir accès.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

Dans le cas où l'Utilisateur accède involontairement à des données qui ne lui sont pas destinées, il lui est demandé – même si ces données ne sont pas expressément protégées – d'en cesser toute prise de connaissance ou de ne pas en prendre connaissance et/ou de cesser toute intrusion dans le système auquel il aura accédé involontairement, notamment suite à une faille du système ou de sa sécurité. Dans ce dernier cas, l'Utilisateur devra signaler immédiatement l'anomalie constatée au support informatique.

Ces données et fichiers informatiques visés comprennent notamment les courriers électroniques.

Les supports de stockage amovibles (tels que notamment les clés USB) permettent non seulement la reproduction des données qu'ils contiennent mais aussi leur modification ou leur altération (en cas d'accident ou de malveillance). En conséquence la copie de données de l'entreprise, en particulier bancaire ou à caractère personnel, est interdit. Dans le cas où ce type de support de stockage est indispensable, il est recommandé à l'Utilisateur de se rapprocher de sa hiérarchie ou du Responsable de la Sécurité des Systèmes d'Information de la Société pour convenir de mesures de protection particulières.

ARTICLE 4 : ACCES A INTERNET

Sur demande du responsable hiérarchique habilité, la Société peut être amenée à fournir aux Utilisateurs un accès à internet à des fins essentiellement professionnelles.

La consultation, la diffusion, l'impression, le traitement de documents, informations, fichiers ou données qui peuvent être qualifiés de frauduleux, illicites, ou qui présenteraient un des caractères listés à l'article 2.4(a), ainsi que la participation à des jeux présentant l'une des caractéristiques contraires aux valeurs du Groupe, sont interdits.

Des centaines de milliers de sites potentiellement « dangereux » sont automatiquement filtrés (la liste de ces sites est régulièrement mise à jour).

Les gestionnaires du système d'information gèrent le filtrage des flux internet entrants et sortants ainsi que les types de fichiers téléchargeables. Il est rappelé que l'Utilisateur ne doit pas modifier les paramètres de sécurité du navigateur sur son Poste.

L'Utilisateur s'interdira de télécharger un programme (shareware, freeware, etc.) afin de l'installer sur son Poste, sauf autorisation préalable par un gestionnaire des systèmes informatiques. Les fichiers dont le téléchargement a été préalablement autorisé restent toutefois soumis au respect des droits d'auteur et de licence.

Si l'Utilisateur a un besoin spécifique, il devra en effectuer la demande conformément à la procédure en vigueur dans l'Entreprise, l'Utilisateur n'étant pas autorisé à modifier les composants des systèmes d'information, conformément à l'article 3 de la présente charte.

L'Utilisateur est informé que, notamment pour des nécessités de maintenance, de sécurité du système d'information et de gestion technique, les échanges via le réseau Carrefour peuvent être analysés et contrôlés dans le respect de la législation en vigueur. En particulier, les fichiers de journalisation des traces de connexion globale sont conservés pendant un an, sauf cas exceptionnels (ex : notification d'un contentieux). Ces fichiers contiennent notamment le nom, l'heure, le jour et l'adresse internet du site visité.

L'Utilisateur est également informé que l'utilisation des ressources informatiques et les échanges via le réseau Carrefour peuvent être enregistrés, l'éventuelle utilisation de ces traces étant conforme à la législation en vigueur.

Il est rappelé à l'Utilisateur que les règles d'utilisation de l'accès à internet ci-dessus s'appliquent également pour un accès à partir de postes nomades mis à disposition par l'Entreprise, que cette utilisation soit faite dans ou hors des infrastructures du Groupe.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

ARTICLE 5 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE ET DES TRANSFERTS DE FICHIERS

Les outils de messagerie électronique et de transfert de fichiers sont mis à la disposition de l'Utilisateur par la Société essentiellement à des fins professionnelles, dans le cadre des fonctions exercées dans l'Entreprise.

Leur utilisation doit être conforme aux dispositions de la présente charte.

Le message électronique est un écrit pouvant engager la Société, le Groupe, voire son auteur à titre individuel. Il peut être reconnu comme preuve valable pour établir un fait ou un acte juridique. Chaque Utilisateur doit donc porter une attention toute particulière à la rédaction d'un courriel et à sa diffusion.

Les risques d'erreurs, de divulgation d'information et d'atteinte à l'image de marque de la Société ou plus globalement du Groupe imposent la plus grande prudence. Il incombe à tout Utilisateur de veiller à préserver toute information à caractère confidentiel relevant de l'activité professionnelle ou de la vie privée détenue par la Société ou par le Groupe (exemple : données à caractère personnel en matière de gestion des ressources humaines).

Chaque Utilisateur doit notamment vérifier rigoureusement l'adresse des destinataires lors de l'envoi d'un message à l'extérieur de l'Entreprise.

Afin d'éviter la dégradation des performances des Ressources Informatiques, l'Utilisateur doit veiller à appliquer les recommandations suivantes :

- Le transfert et le partage de fichiers doivent être effectué avec les moyens mis à disposition par le Groupe:
  - Transfert de fichiers volumineux avec l'extérieur, FileExchange
  - Partage de fichiers avec l'extérieur, FileConnect
  - Partage de fichier en interne Google Drive

- L'utilisation d'espaces de stockage ou d'échange de fichiers non homologués par le groupe est proscrit, (sauf exceptions validées par le Responsable Sécurité du Système d'Information).

- réduire au strict minimum la taille et le nombre des documents attachés ;

- ne pas utiliser les logos, fichiers, images ou animations dans les signatures automatiques, car ceux-ci augmentent inutilement la taille des courriels ;

- adresser les courriels aux seuls destinataires réellement concernés par leur contenu et éviter les mises en copie ainsi que les demandes d'accusé de réception systématiques ;

- éviter d'utiliser la fonction « répondre à tous » lorsqu'il y a de nombreux destinataires et veiller, lors de l'utilisation de la fonction « répondre avec historique », à supprimer les fichiers attachés d'origine ;

- ne pas faire suivre mais détruire les messages du type « chaîne de solidarité » ou « canulars » ;

- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir le service support Utilisateurs ;

- supprimer sans les ouvrir les messages suspects c'est-à-dire présentant une ou plusieurs caractéristiques laissant supposer un risque pour la sécurité des systèmes d'information.

Toute utilisation de la messagerie à des fins de promouvoir ses activités personnelles à caractère commerciales ou non personnelles ou en lien avec ses opinions personnelles est interdite (sauf accord exprès de la Direction de l'Entreprise).

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

L'Utilisateur ne doit jamais envoyer des messages en masse (plus de 20 destinataires, hors diffusion pour raison de service) ou en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement) sauf demande expresse de la Direction. Les informations diffusées via la messagerie engagent la responsabilité civile et/ou pénale de leur auteur.

L'Utilisateur s'interdit de recourir à des procédures automatiques de renvoi de courriels à destination d'une messagerie externe.

ARTICLE 6 : UTILISATION DES RESSOURCES INFORMATIQUES A DES FINS EXTRA-PROFESSIONNELLES, NOTAMMENT UTILISATION A DES FINS PRIVEES, PARTICIPATION A DES RESEAUX SOCIAUX

Article 6.1 : Utilisation des Ressources Informatiques à des fins extra-professionnelles, notamment utilisation à des fins privées

L'utilisation des Ressources Informatiques à des fins privées est tolérée, dès lors qu'elle :

- est conforme aux dispositions de la présente charte ainsi qu'aux lois et règlements applicables ;
- ne présente aucune des caractéristiques listées à l'article 2.4(a) ;
- est limitée et raisonnable, notamment dans le cadre des nécessités de la vie courante et familiale ;
- ne perturbe pas la disponibilité des Ressources Informatiques ;
- n'entrave pas la sécurité (notamment informatique) de l'Entreprise et la qualité de travail de l'Utilisateur ;
- n'implique pas, par rapport à une utilisation professionnelle, d'obligation supplémentaire pour la Société et/ou le Groupe ;
- ne porte pas atteinte aux droits et intérêts de la Société et/ou du Groupe, ou d'autres Utilisateurs.

Dans les conditions autorisées par la loi, et notamment afin de préserver, de manière justifiée et proportionnée, les intérêts légitimes de la Société et/ou du Groupe, le droit dérogatoire d'utiliser les Ressources Informatiques à des fins privées pourrait être suspendu à tout moment, temporairement ou définitivement, individuellement ou globalement, si l'Entreprise constate des abus ou pour tout motif lié à la sécurité ou à la préservation de ses intérêts.

a. Utilisation de la messagerie électronique

Si l'Utilisateur fait usage du droit dérogatoire d'utiliser la messagerie électronique à des fins privées, il est tenu :

- d'indiquer, dans l'objet de tout message électronique, son caractère personnel en indiquant les mentions « Privé » ou « Personnel » et d'inviter ses correspondants à faire de même (à défaut d'une telle mention, le message électronique sera réputé à caractère professionnel et ne bénéficierait pas, conformément à la loi et à la jurisprudence applicables, de la protection réservée aux correspondances privées). Il est rappelé que l'utilisation du terme « privé » ou « personnel » dans le titre d'un mail ou d'un fichier ne doit concerner que des messages à caractère réellement personnel et non pas professionnel.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

- d'éviter toute indication qui pourrait laisser croire à son destinataire que le message est rédigé dans le cadre de l'exercice professionnel ;

- de classer ses courriers électroniques privés (reçus ou envoyés) dans un répertoire à part portant la mention « Privé » ou « Personnel » de manière à prévenir les gestionnaires de la messagerie électronique de la nature particulière des informations qu'il contient. Les gestionnaires de la messagerie s'interdiront la lecture de tels messages, sauf à y être autorisés conformément à la loi (par exemple demande par une autorité etc.).

Le nombre et le volume de messages électroniques mentionnés « Privé » ou « Personnel » ne doivent pas dépasser un nombre et un volume raisonnables.

Les gestionnaires du système d'information peuvent demander à tout Utilisateur d'effacer tout ou partie de ses messages extraprofessionnels présents dans les systèmes d'information de l'Entreprise. En cas d'urgence ou dans le cas où l'Utilisateur ne donne pas suite dans les 24 heures suivant la demande, les messages sortant signalés comme « privé » ou « personnel », les messages identifiables par leur mention « privé » ou « personnel » pourront être effacés par l'administrateur du système d'information sans nouvel avertissement préalable.

Sauf accord exprès et exceptionnel de la Direction, il est interdit de recourir à partir de son poste de travail et via une connexion internet (même dans le cas où cette connexion est autorisée) à un « webmail » dans le but d'accéder ou d'aller chercher ses messages extraprofessionnels dans une messagerie privée. Cette interdiction est fondée sur la prévention du risque - réel et fréquent - d'introduction de virus dans le Système d'Information à partir de messageries privées externes insuffisamment protégées.

b. Usage d'internet

Le nombre et la durée de connexions à caractère extraprofessionnel ou privé à internet ne doivent pas dépasser un nombre et une durée de connexion raisonnables.

c. Stockage de données

Si l'Utilisateur est amené à stocker, à titre exceptionnel et dans des proportions raisonnables, sur le disque dur ou support de stockage de son Poste, ou sur d'autres supports de stockage des Ressources Informatiques, des documents, informations, fichiers ou données qui relèvent de sa vie privée et qui ne sont pas d'ordre professionnel, il devra créer un répertoire portant le nom « Privé » ou « Personnel » et insérer dans ce répertoire lesdits documents, informations, fichiers ou données (à défaut d'une telle mention, lesdits documents, informations, fichiers ou données seront réputés à caractère professionnel et ne bénéficieraient pas, conformément à la loi et à la jurisprudence applicables, de la protection réservée à la vie privée).

d. Absences, départ de l'Entreprise, autres cas particuliers

Chaque Utilisateur doit se conformer à la procédure ci-dessous :

- L'accès au compte de messagerie d'un Utilisateur par un autre Utilisateur exige son accord préalable écrit. Cet accord sera donné pour une durée limitée et à des fins professionnelles spécifiques (ex. prise en charge pendant les congés, collaboration sur un projet) ;

- En cas d'absence ou de congés imprévus notamment (et sans préjudice des droits d'accès dont dispose l'Entreprise conformément à la loi et la jurisprudence applicables), ou lorsqu'il est impossible d'informer préalablement l'Utilisateur et/ou d'obtenir un accord préalable écrit (congé maladie par exemple), l'Entreprise pourra accéder aux données/ informations/ fichiers liées à la continuité de l'activité de l'Entreprise, conformément à la législation applicable et sous le contrôle de la Direction des ressources humaines qui en informera l'Utilisateur ;

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

- Les stagiaires et sous-traitants/ contractants de l'Entreprise (compte de messagerie stagiaires et contractants) et autres tiers ne pourront en aucun cas accéder aux comptes de messagerie des salariés de l'Entreprise ;

- Quand un Utilisateur quitte l'Entreprise, il est tenu d'effacer tous ses contenus, fichiers et données à caractère privé avant de restituer à l'Entreprise les moyens techniques et plus généralement les Ressources Informatiques qui lui ont été confiés par l'Entreprise. A compter de la date de départ de l'Utilisateur, son compte de messagerie sera annulé et tous les messages sous ce compte de messagerie seront transférés selon les procédures internes de l'Entreprise à une personne désignée, afin d'assurer la continuité de l'activité.

L'Entreprise ne sera en aucun cas tenue pour responsable lorsque des données privées qui n'ont pas été effacées par l'Utilisateur auront pu être lues par le nouveau titulaire du poste ou toute personne désignée pour traiter les informations des comptes de messageries des personnes ayant quitté l'Entreprise. Dans tous les cas, l'Utilisateur qui accède accidentellement aux données privées d'un autre Utilisateur doit contacter immédiatement sa Direction des ressources humaines.

Article 6.2 : Réseaux sociaux, forums de discussion externes

Carrefour Banque a pleinement conscience de l'influence actuelle des plates-formes sociales en ligne, telles que les blogs, les wikis, les réseaux sociaux et tous les autres médias sociaux utilisés au sein du Groupe comme à l'extérieur, sur la façon dont nous interagissons. La collaboration en ligne nous permet de partager nos connaissances et nos idées, quel que soit notre statut, notre fonction ou notre expérience. C'est une façon pour nous de participer aux conversations autour des expertises de Carrefour Banque.

Comptes personnels

Lorsque vous créez vos propres comptes réseaux sociaux, vous devez déterminer si vous allez les utiliser pour des contenus personnels, professionnels ou les deux.

Vous pouvez choisir d'avoir des comptes de médias sociaux qui sont entièrement personnels : aucune mention de votre employeur, aucun partage de contenu de l'Entreprise et du Groupe, aucun lien entre votre compte et la marque Carrefour Banque. Dans ce cas, vous êtes libre d'utiliser votre canal comme vous le souhaitez.

Cependant n'oubliez pas, il est presque impossible de dissocier le privé du professionnel. Ce n'est pas parce que vous ne déclarez pas votre employeur qu'il est difficile de faire le lien. Cela signifie qu'en tant qu'employé de Carrefour Banque, nous attendons de vous que vous respectiez notre code d'éthique professionnelle dans tout ce que vous faites.

Comptes professionnels

Dès que vous utilisez un compte réseau social ou un blog qui relie votre contenu à celui de Carrefour Banque, vous devez respecter des règles spécifiques :

- Vous pouvez déclarer votre poste au sein de Carrefour Banque dans votre biographie d'utilisateur, mais il est évident que votre compte n'est pas un canal d'entreprise mais plutôt la voix d'un individu.
- Une fois que vous avez déclaré votre appartenance à Carrefour Banque, tout ce que vous publiez doit refléter nos valeurs et être conforme à nos principes éthiques.
- N'incluez pas Carrefour Banque dans votre profil ou votre nom d'utilisateur (par exemple, @JaneCarrefour-Banque).
- Veuillez ne pas utiliser la marque Carrefour Banque pour votre avatar ou photo de profil. Vous pouvez utiliser les bannières officielles de la marque Carrefour Banque pour vos profils réseaux sociaux.
- Les retweets ou les partages vous engagent personnellement (indépendamment du contenu de votre biographie), ce qui signifie que le partage de contenu pouvant constituer une violation des DPI (Droits de Propriété Intellectuelle), une diffamation, un dénigrement ou un abus ne sera pas toléré.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

- Ne jamais partager un contenu qui est confidentiel pour le client ou qui relève de la propriété

Si vous avez le moindre doute sur la nature appropriée ou non d'un contenu à partager en ligne, ne le publiez pas. Mieux vaut prévenir que guérir.

Responsabilité

Vous êtes personnellement responsable de vos paroles et de vos actes, où que vous vous trouviez, y compris en ligne. N'oubliez pas que lorsque vous participez à une conversation sur un réseau social, vous vous exprimez en tant qu'individu et non au nom du Groupe. Utilisez la première personne du singulier.

Dès lors que vous abordez en ligne des sujets touchant de près ou de loin au Groupe, jouez la carte de la transparence en déclinant votre nom et votre fonction et en précisant que vous travaillez pour le Groupe. Si vous possédez un site personnel faisant référence au Groupe ou ayant une incidence sur celui-ci, insérez une décharge de non-responsabilité telle que « Les opinions exprimées sur ce site sont purement personnelles et n'implique en aucun cas Carrefour Banque ou Carrefour. »

Dans la mesure autorisée par la loi en vigueur, sachez que le Groupe et l'Entreprise se réserve le droit de surveiller le recours aux plates-formes sociales et collaboratives et de prendre les mesures appropriées dans le but de se protéger contre toute utilisation abusive susceptible de nuire à sa réputation. Les infractions à ces lignes directrices peuvent être sanctionnées selon la politique locale des ressources humaines, conformément aux lois applicables.

La création d'un compte au nom du Groupe ou de l'Entreprise ou la nomination en tant que représentant officiel habilité à partager des informations sur le Groupe et/ou l'Entreprise et ses domaines d'intervention nécessite l'autorisation préalable du Groupe et/ou de l'Entreprise ou de ses équipes marketing et communications. Seuls les comptes approuvés sont autorisés à afficher le logo de l'entreprise. Si vous souhaitez représenter Carrefour Banque ou créer un compte pour Carrefour Banque, veuillez contacter votre équipe marketing et communications locale ou l'équipe Web de l'Entreprise. Si la presse ou des médias en ligne vous contactent au sujet d'un contenu en ligne concernant Carrefour Banque, veuillez l'inviter à contacter le service communication ou votre responsable des ressources humaines local.

Conduite irréprochable

Votre comportement en ligne doit être conforme à notre Charte de déontologie. Vous avez la possibilité de contribuer à façonner la réputation du Groupe et/ou de l'Entreprise en ligne. Utilisez vos connaissances d'expert pour enrichir les discussions, aider à résoudre les problèmes, partager l'enthousiasme de notre environnement de travail, promouvoir l'apprentissage et le partage d'idées.

La confiance est la clé pour établir des relations en ligne. Établissez une relation de confiance en gardant un ton respectueux, y compris lorsque vous contestez les propos d'autres personnes et en répondant aux commentaires de manière opportune. Si vous vous rendez compte que vous avez fait une erreur, essayez de la corriger rapidement.

N'adoptez aucun comportement en ligne qui ne serait pas acceptable sur votre lieu de travail ou qui serait contraire à la loi. Par exemple, ne faites aucune remarque désobligeante, ne vous livrez à aucune tentative de maltraitance, d'intimidation ou de harcèlement, ne proférez aucune insulte ou ne publiez aucun contenu à caractère haineux, diffamatoire, menaçant, discriminatoire ou encore pornographique.

Carrefour Banque tient compte des opinions personnelles de chacun et vous devez respecter les autres et leur droit de penser différemment de vous. Il convient de rappeler que les sujets impliquant la politique, la religion et la sexualité peuvent être très sensibles et vous devez envisager de vous abstenir d'aborder certains sujets qui seraient considérés comme personnels, répréhensibles ou même offensants. Vous ne devez pas faire de remarques, de plaisanteries ou afficher du contenu qui pourrait offenser un membre d'une race, d'une religion ou d'un sexe particulier.

Gardez également à l'esprit que vos lecteurs, en raison d'un manque de communication non verbale ou de différences culturelles, peuvent interpréter vos contenus partagés en ligne de différentes manières. Certains

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

utilisateurs peuvent ne pas être familiers avec les abréviations, les émoticônes et autres codes courants utilisés dans les communications en ligne. N'oubliez pas non plus que les commentaires sont souvent pris hors contexte, alors tenez-vous en aux faits.

Respect de la confidentialité

Veillez à protéger constamment les données confidentielles et toute autre information propriétaire relatives aux clients, au Groupe et/ou de l'Entreprise et aux fournisseurs. Ne publiez aucun contenu en ligne que vous ne partageriez avec un journaliste, un client, un analyste ou un concurrent.

Assurez-vous que les références, quelles qu'elles soient, aux clients, partenaires et fournisseurs, n'enfreignent aucun accord de confidentialité. Veuillez également tenir compte des clauses de confidentialité que vous avez signées dans votre propre contrat de travail.

Ne divulguez aucune information à propos de vos collègues ou toute autre personne, n'utilisez pas leurs données de façon inappropriée et ne publiez jamais leurs photos sans leur autorisation.

Même dans le cas d'une application à signature unique (comme Currents, Confluence, HangOut, etc.), nous recommandons aux utilisateurs de faire preuve de bon sens en ce qui concerne les informations de nature sensible. Ne partagez aucune information confidentielle concernant les clients, le Groupe et/ou de l'Entreprise ou les fournisseurs sur les plates-formes sociales et collaboratives si leur accès n'est pas limité à une communauté restreinte étroitement contrôlée, dont les participants ont été autorisés à recevoir des informations de cette nature et si lesdites plates-formes ne sont pas équipées des niveaux de sécurité appropriés. Les sites publics ne sont pas appropriés à la publication de communications internes entre les employés du Groupe et/ou de l'Entreprise.

Protection des droits d'auteur

Respectez les lois et les réglementations en vigueur, et plus particulièrement les lois régissant les droits de propriété intellectuelle, les droits d'auteur et les marques commerciales.

Vous n'êtes pas autorisé à publier du contenu ni à prendre des mesures contraires à la loi ou enfreignant les droits de propriété intellectuelle du Groupe et/ou de l'Entreprise ou de toute tierce partie.

Concernant les marques Carrefour Banque, en plus des règles décrites dans ce document, vous devez respecter la politique de marque du Groupe et/ou de l'Entreprise et les directives relatives à l'identité visuelle.

ARTICLE 7 : VIGILANCE DE CHAQUE UTILISATEUR

En cas d'anomalie lors de l'utilisation des applications communicantes (accès à internet, messagerie, transfert de fichiers etc.) et des supports de stockage (CD-Rom, supports de stockage amovibles, etc.), l'Utilisateur doit stopper toute transaction et prévenir immédiatement le service de support informatique approprié ou le Responsable de la sécurité informatique.

En outre, il est demandé à chaque Utilisateur de signaler toute tentative de violation de son Poste ou de ses fichiers ou données, dès qu'il en a connaissance, auprès de sa hiérarchie ou du Responsable de la Sécurité du Système d'Information de l'Entreprise.

ARTICLE 8 : MOYENS DE CONTROLE ET AUDITS

La Société se réserve la possibilité d'effectuer des vérifications et contrôles et de procéder à des audits de la bonne application de la présente charte et plus généralement du respect par les Utilisateurs des règles applicables, le tout dans les limites prévues par la loi, notamment en ce qui concerne les libertés individuelles des Utilisateurs.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

Des analyses et des contrôles pourront notamment être effectués sur l'utilisation des Ressources Informatiques :

- pour des raisons de maintenance et de gestion technique, et en particulier afin d'optimiser les ressources. En effet, certains types de messages sont souvent à l'origine d'incidents (problème espace disque, encombrement du réseau, diffusion en chaîne, « cookies », etc.) ;

- pour se prémunir contre une utilisation non conforme des Ressources Informatiques pouvant entraîner notamment une altération de l'image de marque du Groupe ou des problèmes de sécurité.

Ces analyses sont susceptibles d'être réalisées, par sondage ou en fonction d'éléments indiquant une utilisation contraire aux règles applicables.

Des contrôles a posteriori peuvent être réalisés sur l'usage de la messagerie. Ils portent en particulier sur :

- les volumes/nombre de messages échangés ;

- les tailles des messages (par exemple supérieures à 1 Mo, comprises entre 1 et 2 Mo, supérieures à 2 Mo) ;

- le format des pièces jointes (images, vidéos, exécutables, fichiers compressés, etc.)

- la quantité d'espace disque utilisée ;

- une analyse sémantique des messages (sélection de mots à caractère pornographique, raciste, etc.).

Au niveau du pare-feu (ou firewall), l'entreprise aura la possibilité de vérifier le trafic sortant et entrant dans l'entreprise. Sont détenues toutes les traces de l'activité qui transite par le pare-feu (sites visités, heures des visites, éléments téléchargés, nature du texte, images, vidéos ou logiciels).

Des contrôles a posteriori peuvent ainsi être réalisés sur l'usage d'internet, ils portent sur :

- la durée de connexion,
- les volumes transférés,
- les sites visités.

Un outil permettant d'analyser les contenus des sites visités et de filtrer l'accès à certains sites (liste noire) est mis en place : sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

L'Entreprise attire l'attention de chaque Utilisateur sur le fait que les outils informatiques génèrent aujourd'hui automatiquement des traces, sans que celles-ci aient été spécifiquement conçues pour permettre d'exercer une surveillance ; même si certaines de ces données peuvent être utilisées à des fins de contrôle, tel qu'indiqué ci-dessus. Même dans le cas où les technologies ou les configurations peuvent le permettre, l'Utilisateur s'interdit d'effacer toute trace liée à son activité.

D'une manière générale, l'Utilisateur admet que toute connexion aux réseaux internes de l'Entreprise l'identifie et qu'elle est une acceptation de l'enregistrement automatique de traces de son activité.

ARTICLE 9 : SANCTIONS

Le non-respect des règles et mesures de sécurité figurant dans la présente charte engage la responsabilité personnelle de l'Utilisateur, dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose, éventuellement et de manière appropriée et proportionnée au manquement commis, aux sanctions disciplinaires définies par le règlement intérieur.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

La procédure disciplinaire et les sanctions resteront de la compétence de l'entreprise qui emploie toutes personnes extérieures intervenant au sein de la Société à quelque titre que ce soit.

L'Utilisateur est seul responsable de l'utilisation des Ressources Informatiques qui lui sont confiées ou auxquelles il a accès et ce, notamment lorsque cette utilisation va à l'encontre des dispositions prévues par la présente charte (accès à des sites illicites etc.).

Dans l'hypothèse où l'Utilisateur engagerait tout de même la responsabilité civile ou pénale de la Société, cette dernière pourrait exercer un recours contre l'Utilisateur responsable conformément au droit commun.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.

ANNEXES

Annexe 1 : Règle de Classification des Données

Une Information sensible, est une information dont la compromission, l'altération, le détournement, la destruction ou plus généralement la diffusion intempestive est de nature à nuire à la continuité des activités de l'entreprise en situation normale comme en situation de crise, et peut engendrer des pertes financières ou un impact certain en termes d'image.

De manière générale, l'information sensible (en matière de confidentialité) pour le Groupe Carrefour relève de huit domaines spécifiques :

- Les données financières
- Les données commerciales ayant une criticité particulière pour l'activité de Carrefour
- Les données à caractère personnel
- Les données associées aux clients Carrefour
- Les données juridiques
- Les données stratégiques
- Les données caractérisant un savoir-faire du Groupe Carrefour
- Les données sécurité

Pour les besoins de la gestion de la confidentialité de l'information sensible, il existe deux niveaux de protection hiérarchiques : CONFIDENTIEL, INTERNE :

Classification	Objectif
CONFIDENTIEL Carrefour	***Protéger en interne les informations vitales et stratégiques pour Carrefour*** • La divulgation de telles informations pourrait affaiblir la position du Groupe Carrefour dans son ensemble ou aboutir à des pertes financières conséquentes. • La nature de ces informations est telle que leur diffusion non autorisée pourrait avoir un sérieux impact sur l'entreprise, ses actionnaires, ses partenaires commerciaux ou ses clients.
INTERNE Carrefour	***Protéger de l'extérieur les informations du Groupe Carrefour dont la diffusion externe n'est pas souhaitable*** • Ces informations peuvent être diffusées librement auprès du personnel de l'entreprise. En principe, leur diffusion non autorisée n'est pas susceptible de nuire à l'entreprise, ses actionnaires, ses partenaires commerciaux ou ses clients. Toutefois, un manipulateur sera susceptible d'exploiter ces informations par recoupement. Pour ce niveau, il n'est pas demandé de marquage particulier.

Chacun de ces deux niveaux peut être complété par une limitation particulière du « besoin de connaître ». Une personne, même suffisamment habilitée pour accéder à une information classifiée, ne pourra accéder à cette information que si elle a besoin de connaître cette information pour le travail qu'elle a à réaliser.

La classification ou la dé-classification d'une information ainsi que l'application des règles de création, de marquage, de sauvegarde et de transmission de l'information sont de la responsabilité de son propriétaire.

Les utilisateurs de l'information sont responsables de l'application des règles de conservation de l'information.

Ce document contient des informations confidentielles, appartenant à Carrefour Banque. Toute divulgation, utilisation, diffusion ou reproduction totale ou partielle de ce document, ou d'informations qu'elle contient, doit être préalablement autorisée par Carrefour Banque.