I. Préambule

La présente charte s'inscrit dans le cadre des politiques du Groupe Hutchinson en matière :

- de sécurité des systèmes d'information,
- de sécurité et de santé des collaborateurs,
- d'éthique et de conformité.

Elle est conforme au contexte législatif et réglementaire français en vigueur et évoluera en fonction de ce contexte et des politiques du Groupe. Cette charte informatique s'impose à tous les utilisateurs du système d'information et de communication du Groupe Hutchinson, tels que définis ci-dessous.

Le Groupe Hutchinson utilise des ressources informatiques et de télécommunication dont la sécurité et le bon usage constituent des enjeux majeurs. Des moyens appropriés pour protéger ces ressources et leurs utilisateurs sont mis en œuvre.

En effet, le groupe a mis en œuvre les moyens humains et techniques appropriés, matériels et logiciels, pour son système d'information et de communication. À ce titre, il lui appartient d'acquérir les équipements et licences à jour nécessaires à l'utilisation des ressources mises à la disposition des utilisateurs.

Tout utilisateur (salarié, personnel intérimaire, stagiaire, prestataire, partenaire, invité, …) des ressources informatiques et de télécommunication du Groupe doit contribuer à leur bon usage et à leur sécurité dans le respect des neuf grands principes et des exigences définis par la présente charte.

L'utilisateur est responsable des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à leur protection. L'utilisateur doit veiller à la protection des équipements contre le vol et les dégradations. Il doit veiller à la protection des données. Les données confidentielles doivent être chiffrées suivant les modalités fixées par le Groupe.

II. Champ d'application

La présente charte s'applique dans toutes les sociétés du Groupe Hutchinson aux utilisateurs du système d'information et de communication dudit Groupe, dans le respect des règles de décision propres à chacune de ces sociétés et sous réserve des dispositions légales et règlementaires applicables localement.
Il revient aux hiérarchies de veiller à ce que la règle soit connue, comprise et appliquée par tout utilisateur.

Par ailleurs, tout accord passé avec un tiers donnant accès aux données, aux ressources informatiques et de communication du Groupe, devra stipuler que le tiers, y compris son personnel, ses sous-traitants et toute personne intervenant sous sa responsabilité, s'engage à respecter la présente Charte ou sa déclinaison locale.

III. Définition du système d'information et de communication

Le système d'information et communication du groupe Hutchinson est notamment constitué des éléments suivants :

- les infrastructures informatiques (espaces de stockage, serveurs applicatifs, serveurs d'accès à distance aux Services, systèmes de sécurité…) et réseaux de communications électroniques,
- les ordinateurs (fixes ou mobiles), smartphones, tablettes et tout autre équipement informatique professionnel (c'est-à-dire délivré par le Groupe),
- les périphériques, à savoir les imprimantes, photocopieurs, fax, clés USB, disques durs externes, délivrés par le Groupe,
- les logiciels, progiciels, bases de données ainsi que les fichiers, utilisées par le Groupe,
- les services de communication téléphonique et électronique, fixes ou mobiles et les abonnements associés,
- la messagerie électronique, l'intranet et/ou l'extranet, les applications informatiques,
- les habilitations informatiques fournies par le Groupe permettant aux utilisateurs d'accéder au système d'information,
- les services Cloud, dès lors qu'ils font l'objet d'un contrat avec le Groupe.
- Le matériel personnel des salariés contenant des informations à caractères professionnel et dés lors que la configuration permet l'accès au système d'information du Groupe.

Les éléments du système d'information et de communication mis à disposition d'un employé, appartiennent au Groupe Hutchinson et peuvent à tout moment être réaffecté à un autre salarié.

IV. Objet de la charte

Cette charte a pour objet de préciser les droits, les devoirs et les responsabilités des utilisateurs, en accord avec la législation.
Elle n'a pas pour objet de couvrir de façon exhaustive tous les cas de figure possibles mais de fixer des principes généraux d'utilisation, qui ne sont pas exclusifs des règles de courtoisie et de respect d'autrui.
Tous les utilisateurs contribuent à la sécurité des systèmes d'information du groupe Hutchinson dans un climat de loyauté et de confiance réciproque.

V. Principes et exigences

Principe 1 : respect des lois, des règlementations et des exigences du Groupe

Exigence 1.1 : respect des lois et réglementations applicables

L'utilisateur doit respecter la réglementation applicable aux ressources informatiques et de télécommunication, notamment dans les domaines de la communication électronique, de la sécurité informatique, de la protection des données à caractère personnel, de la propriété intellectuelle et de la concurrence.

Exigence 1.2 : respect du référentiel Groupe

Outre le Code de conduite TOTALENERGIES, l'utilisateur doit respecter le référentiel du Groupe, et notamment les règles relatives à :

- la sûreté du patrimoine informationnel,
- la protection des données personnelles,
- la cybersécurité des systèmes d'information d'entreprise et industriels,
- la conservation des documents

Exigence 1.3 : respect des préconisations du Groupe

L'utilisateur doit connaître les préconisations du Groupe qui font l'objet de règles d'usage sous forme de fiches pratiques (guide bonnes pratiques applications) et de guides techniques accessibles sur l'intranet.

Principe 2 : usage privé des ressources informatiques et de télécommunication

Exigence 2.1 : conditions de l'usage privé des ressources

L'utilisateur doit réserver à un usage professionnel les ressources (e-mail, accès internet, usage du téléphone, visioconférence…) que le Groupe met à sa disposition.

Néanmoins, un usage à titre privé, hors temps de travail, peut être admis sous réserve qu'il :

- reste ponctuel et raisonnable,
- ne perturbe pas l'activité professionnelle de l'utilisateur et/ou des autres utilisateurs,
- n'engendre pas une consommation anormale des ressources,
- n'affecte pas le fonctionnement des ressources,
- ne porte pas préjudice au Groupe, et/ou ne porte pas atteinte à son image ou à sa réputation.

Tous les fichiers créés ainsi que tous les messages envoyés par un utilisateur grâce aux ressources mises à sa disposition pour l'exécution de ses missions sont présumés avoir un caractère professionnel sauf si l'utilisateur les identifie comme étant « Personnel » ou « Privé » ou qu'il les a classés dans un dossier identifié comme « Privé » ou « Personnel ».
Afin d'éviter l'interception de tout message destiné à une instance représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

Le Groupe est susceptible d'accéder à tout document ou message professionnel (non spécifié comme personnel/privé), y compris hors la présence de l'utilisateur, dans les limites et conditions prévues par la règlementation applicable.

Pour des raisons de sécurité et du respect de la loi, l'accès à certains sites Internet peut être prohibé par le groupe Hutchinson. De plus, Hutchinson peut imposer la configuration du navigateur et restreindre le téléchargement de certains fichiers ou l'accès à certains fichiers.

Exigence 2.2 : favoriser les moyens de communication et de stockage privés

L'utilisateur doit privilégier, à chaque fois que cela est possible :

- son système de messagerie personnelle pour envoyer des messages personnels,

- ses équipements informatiques et de communication personnels pour stocker des documents personnels.

Le Groupe ne sera, en tout état de cause, pas responsable de la sécurité des données stockées à des fins personnelles sur les ressources du Groupe et ne pourra pas être tenue responsable de la réception d'un message électronique non désiré

Principe 3 : usage professionnel d'équipements n'appartenant pas au Groupe et de services accessibles sur Internet

Ces exigences s'appliquent lorsque l'utilisateur, dans le cadre de ses activités professionnelles pour le Groupe, utilise des équipements n'appartenant pas au Groupe, tels que :

- des équipements personnels,
- des équipements professionnels n'appartenant pas au Groupe ou non remis par le Groupe (équipements des prestataires…).

Exigence 3.1 : condition d'autorisation préalable de l'usage à des fins professionnelles d'équipements n'appartenant pas au Groupe

A l'exception de systèmes ou services conçus explicitement par la direction informatique pour accepter l'utilisation de tels équipements, l'utilisation à des fins professionnelles d'équipements n'appartenant pas au Groupe ou non remis par le Groupe, est soumise à une autorisation préalable. Cette autorisation peut être conditionnée à un périmètre : projet, opérations particulières, durée, etc.

Il est strictement interdit à l'utilisateur d'utiliser des équipements personnels ou n'appartenant pas au Groupe (exemple tablette, téléphone portable personnels, etc.) à des fins professionnelles en dehors des applications préconisées par le groupe.

Exigence 3.2 : responsabilité de l'utilisateur sur des équipements n'appartenant pas au Groupe lorsqu'ils sont utilisés à des fins professionnelles pour le Groupe

L'utilisateur est responsable de :

- la conservation, l'utilisation de ses équipements personnels, le cas échéant de son/ses abonnement(s) à un réseau de communication électronique ou téléphonique, de ses applications et de ses données,
- la configuration de sécurité de ses équipements nécessaire à l'accès aux ressources (conformité aux contrôles automatiques mis en place par le Groupe),
- l'utilisation conforme de la configuration et des logiciels mis à sa disposition par le Groupe et installés sur ses équipements personnels autorisés ainsi que du respect des règles de protection des données du Groupe,
- toute destruction, perte, altération, accidentelle ou résultant d'un acte de malveillance (vol, ransomware, virus, etc.), y compris en cas de défaut ou d'insuffisance de sécurisation de son/ses équipement(s) personnel(s) (à l'exception des configurations d'accès réalisées par le Groupe dès lors qu'elles ne sont pas modifiées par l'utilisateur),
- signaler immédiatement tout vol ou perte de ses équipements, afin que le Groupe puisse prendre les mesures conservatoires adéquates.

Exigence 3.3 : usage de services numériques disponibles sur internet n'appartenant pas au Groupe

L'utilisateur s'interdit par ailleurs, sauf obtention d'une autorisation préalable :

- tout usage à des fins professionnelles des services disponibles sur Internet, y compris les applications mobiles disponibles publiquement depuis des « App stores »,
- toute création de nouvelles ressources (tel qu'un site web réalisé à des fins professionnelles)

Les autorisations ne peuvent être données que par la direction des systèmes d'information du Groupe ou une personne possédant une délégation.

Principe 4 : intégrité des ressources et des habilitations informatiques

Exigence 4.1 : intégrité des ressources : droits et interdictions pour l'utilisateur

L'utilisateur est responsable de son usage des ressources et il doit notamment :

- respecter les configurations standards des équipements qui lui sont fournis par le Groupe : modifier la configuration peut créer des dysfonctionnements ou des failles dans la protection des équipements et peut entraîner la déstabilisation de l'ensemble du réseau,
- s'interdire de connecter au système d'information du Groupe tout équipement personnel non autorisé,
- s'interdire d'accéder à des applications, des données ou à des systèmes pour lesquels il ne dispose pas des droits nécessaires, qu'ils appartiennent au Groupe ou non, sans autorisation préalable,
- s'interdire d'installer tout matériel ou logiciel non autorisé par le Groupe et sans obtention des licences requises, sous peine d'exposer le Groupe à de grands risques de piratage et des risques juridiques.
- s'interdire de désactiver ou contourner les systèmes de sécurité informatique du Groupe (contrôles d'accès, anti-virus et firewall par exemple).

Principe 5 : interdiction de tout usage des ressources pouvant porter atteinte aux intérêts du Groupe

Exigence 5.1 : interdiction de porter atteinte aux intérêts du Groupe

En toutes circonstances, l'utilisateur s'interdit d'entreprendre toute action :

- portant atteinte à l'image de marque interne et/ou externe du Groupe,
- portant atteinte aux droits de propriété intellectuelle du Groupe ou de tiers,
- susceptible d'engager la responsabilité civile et/ou pénale du Groupe.

Exigence 5.2 : les comportements interdits dans le cadre de l'utilisation des ressources

L'utilisateur s'interdit d'utiliser les ressources en violation de la présente charte et notamment de :

- charger, stocker, publier, consulter, diffuser ou distribuer au moyen des ressources du Groupe ou d'autres équipements utilisés dans le cadre professionnel, des contenus tels que des documents, informations, images, vidéos:
  - à caractère violent, pornographique, calomnieux ou contraires aux bonnes mœurs, raciste, discriminatoire, ou susceptible de porter atteinte au respect de la personne humaine et de sa dignité

ou portant atteinte à la protection des mineurs,

- à caractère diffamatoire,
- à des fins de harcèlement, menaces, injures,
- à des fins politiques, religieuses ou confessionnelles, commerciales personnelles ou ludiques et tout agissement visant à obtenir des avantages, des gains ou des profits personnels,
- incitant à commettre un crime ou un délit, ou faisant l'apologie des crimes de guerre ou des crimes contre l'humanité,
- portant atteinte à l'intimité de la vie privée d'autrui ou violant les règles de protection des données personnelles ou les droits de la personnalité et le droit à l'image d'autrui,

- charger, stocker ou transmettre des fichiers, des programmes, logiciels, progiciels (…) en violation des lois sur la protection des données personnelles, de la propriété intellectuelle, des règles de confidentialité ou des exigences techniques définies par le Groupe.
- falsifier tout fichier ou imiter tout en-tête ou tout document, ou encore manipuler des identifiants dans le but de dissimuler l'origine d'un contenu,
- accéder de manière frauduleuse aux comptes d'autres utilisateurs ou usurper une identité (envoi de messages sous une adresse électronique usurpée…),
- tenter de lire, modifier, copier ou détruire toutes autres données que celles qui lui appartiennent ou qu'il conserve pour le compte du Groupe ou auxquelles il a accès légitimement en vertu de ses missions (toute destruction des données devant être conforme à la politique du Groupe en la matière) sans l'autorisation de la personne intéressée. Si un utilisateur se livre par inadvertance à l'une de ces activités, il doit en informer immédiatement le service informatique,
- envoyer des messages en masse (hors diffusion sur des listes de l'entreprise pour raisons de service) ou en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement). Limiter le nombre de destinataires (<50) et ne pas attacher de fichiers trop volumineux (<10 Mo). Consulter le service informatique pour des échanges plus volumineux,
- gêner l'usage fait par d'autres utilisateurs des différentes ressources,
- réaliser un traitement sur des données personnelles contraire à la règlement relative à la protection des données personnelles.
- bloquer le fonctionnement des outils liés au fonctionnement des systèmes d'information.

Par ailleurs conformément à la politique de conversation des données, l'utilisateur doit réaliser l'archivage, le traitement, ou la suppression des messages présents dans sa messagerie électronique professionnelle dans un délai de 90 jours suivant la réception ou l'envoi du message.

Exigence 5.3 : Utilisation des médias sociaux

Lors de l'utilisation des médias sociaux (en ce qui comprend les réseaux sociaux, blogs, forums de discussion, sites de partage de vidéos et de photographies), l'utilisateur est soumis aux exigences de la présente charte que ce soit :

- à titre professionnel, lorsqu'il s'exprime au nom du Groupe Hutchinson ou les utilise dans le cadre de l'exercice de ses activités professionnelles et notamment pour des besoins de communication ou de recrutement,

- à titre personnel, dès lors que le contenu qu'il diffuse concerne le Groupe, son activité, les salariés, dirigeants, partenaires, fournisseurs, clients ou concurrents.

L'utilisateur ne doit en aucun cas communiquer sur les réseaux sociaux, blogs, forums de discussion ou autres des documents confidentiels appartenant au Groupe et d'une façon générale ne communiquer que des informations qui ne soient déjà publiques**.**

En dehors de toute délégation de pouvoirs, l'utilisateur s'interdit toute prise de position publique au nom du Groupe. L'utilisateur a en revanche le droit de s'exprimer en son nom propre mais ne doit pas faire apparaître son appartenance au Groupe (usage du logo Hutchinson ou utilisation de l'adresse de messagerie professionnelle).

Par ailleurs l'utilisateur se comporte de manière loyale, responsable et fait preuve de discernement, de courtoisie, de politesse, de modération et de bon sens lorsqu'il fait usage des médias sociaux.
Hutchinson rappelle donc de respecter les règles figurant dans le guide d'usage des réseaux sociaux mis à disposition sur l'intranet.
Il s'assure donc que le contenu éditorial qu'il met en ligne ne contienne pas de propos désobligeants concernant le Groupe, ses employés, clients, partenaires, fournisseurs ou concurrents.

Principe 6 : respect de la sureté de l'information professionnelle et de confidentialité

Chaque utilisateur respecte les règles définies pour assurer la confidentialité, l'intégrité et la disponibilité ainsi que plus généralement la sûreté des informations professionnelles auxquelles il pourrait avoir accès.

Exigence 6.1 : sûreté des informations

L'utilisateur s'engage à prendre toutes les précautions requises conformément aux préconisations du Groupe, dans le cadre de ses fonctions et de ses prérogatives, afin de préserver la confidentialité, l'intégrité et la disponibilité ainsi que plus généralement la sûreté des informations auxquelles il a accès.
Il s'engage notamment à empêcher toute modification ou altération indue de ces informations ainsi que leur communication à des personnes qui ne sont pas expressément autorisées à les recevoir.

Exigence 6.2 : obligation de confidentialité

L'utilisateur est personnellement responsable du respect de l'obligation de confidentialité de toute information qu'il est susceptible de détenir, de consulter ou d'utiliser. Les règles en matière de confidentialité ou d'autorisation préalable avant la publication ou la diffusion d'informations sont définies par le Groupe et sont applicables quel que soit le moyen de communication utilisé.

Pour garantir la confidentialité des informations, il convient de respecter les règles de bon usage et notamment :

- la classification des informations (c'est-à-dire l'estimation de l'impact sur le Groupe en cas de divulgation) en suivant les règles internes en vigueur, et l'application des règles générales de protection qui en découle,
- les règles spécifiques au domaine de l'informatique dont celles relatives :
  - au chiffrement systématique des données confidentielles par un dispositif validé par le Groupe pour le pays où l'utilisateur se trouve,
  - au strict respect de la confidentialité des moyens d'authentification (non-communication mot de passe dans la messagerie, conservation sécurisée),

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés en clair, sous quelque forme que ce soit. Ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

  - au verrouillage des postes de travail afin qu'aucune personne non autorisée ne puisse avoir accès au poste de travail d'un utilisateur à son insu,
  - à la protection contre les vols et les regards indiscrets : éviter, lors de déplacements, de travailler au vu et au su de tout le monde ; de laisser son portable sans surveillance. Dans les bureaux, attacher les ordinateurs portables avec un antivol ou les mettre sous clés,
- l'interdiction du stockage de données professionnelles sur des équipements personnels sans habilitation préalable.

Principe 7 : encadrement des échanges avec des tiers par les délégations de pouvoirs

L'utilisateur doit être vigilant au fait qu'un échange de messages peut constituer de façon involontaire un contrat ou une reconnaissance de responsabilité qui engage le Groupe.

Exigence 7.1 : respect des délégations de pouvoirs

L'utilisateur doit veiller à respecter les délégations de pouvoir et à ne pas engager le Groupe involontairement.

L'utilisateur doit notamment veiller à ne jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie…) car le message électronique peut :

- constituer une preuve ou un commencement de preuve par écrit pouvant engager le Groupe ou l'une quelconque de ses sociétés ;
- être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant.

Principe 8 : contrôle, audit

Exigence 8.1 : contrôle et audit nécessaires à la sécurité des ressources

Tout utilisateur pourra être contrôlé sur le respect de la présente Charte et de son utilisation des ressources et des outils lui appartenant, dans le strict respect du cadre légal applicable et de la vie privée.
En effet, le Groupe doit se protéger contre les préjudices causés par les actes de malveillance, les défaillances techniques et les erreurs humaines pouvant survenir sur les ressources.

Les dispositifs de contrôle et d'audit visent à protéger le Groupe en supervisant l'utilisation des ressources d'une part, ainsi qu'à s'assurer, dans les limites prévues par la réglementation applicable, du respect des dispositions de la présente Charte par les utilisateurs d'autre part.

Le Groupe met ainsi en place :

- des équipements pour assurer la sécurité globale des réseaux, des données, des applications et des accès aux postes de travail, notamment par le filtrage et l'inspection des flux Internet, et permettant de détecter toute activité malveillante sur les systèmes d'information du Groupe,
- des applications de sécurité, tel que l'antivirus, permettant de détecter la présence de certains programmes malveillants sur les ressources,

- des mécanismes de supervision, permettant de détecter les erreurs matérielles et logicielles, et contrôlant l'accès des utilisateurs et des tiers aux ressources,
- des procédures d'identification individuelle et de protection par des moyens d'authentification permettant d'éviter les usurpations d'identité,
- la conservation, dans le respect de la règlementation applicable, des journaux de données de connexion (notamment relatives à l'utilisation d'applications, aux connexions entrantes ou sortantes du réseau interne, au système de messagerie et à l'Internet, aux appels téléphoniques passés ou reçus à partir de téléphones fixes ou mobiles ainsi que les données liées aux messages instantanés).

Dans le cadre de l'utilisation d'équipements n'appartenant pas au Groupe, l'utilisateur est informé que peuvent être réalisés sur les équipements :

- des contrôles automatiques de sécurité afin de permettre l'accès aux ressources (niveau de mise à jour, présence d'un anti-virus à jour, etc.) ;
- des effacements de configurations d'accès distants et des données :
  - en cas de perte, de vol, d'endommagement (notamment si l'équipement de l'utilisateur doit être réparé par un tiers ou mis au rebut), de revente, prêt ou de tout évènement faisant perdre la maîtrise exclusive de son équipement à l'utilisateur ou si l'utilisateur pense que son équipement a pu être corrompu (perte de confidentialité, identifiants volés, etc.). L'utilisateur doit, dès qu'il en a connaissance, en informer dans les plus brefs délais le service informatique du Groupe ;
  - en cas de détection d'une activité frauduleuse ou présumée comme telle.

L'utilisateur est en outre informé qu'en cas d'incident ou de suspicion d'incident de sécurité relatifs à un équipement n'appartenant pas au Groupe (habilité ou non), des analyses techniques pourront être réalisées par le Groupe sur ses équipements. L'utilisateur devra alors remettre à première demande ses équipements aux fins de l'analyse.

Bonne pratique pour éviter les tentatives de fraude, hameçonnage :

Si en tant qu'utilisateur vous avez un doute sur un mail, voici des points à contrôler :

- Pour repérer un e-mail de phishing il faut étudier la source →penchez-vous sur l'expéditeur.
  - Si vous ne le connaissez pas, étudiez l'adresse de plus près.
  - Ne regardez pas uniquement le nom qui s'affiche. Observez l'adresse et le domaine. Ont-ils l'air suspects ?
  - Un soupçon peut être subjectif, mais certains signes sont évocateurs : fautes d'orthographe, chaînes de lettres et de chiffres incompréhensibles, incohérence entre les noms affichés et l'adresse e-mail (mailto).

- Soyez à l'affût de ces signes, car ils peuvent vous aider à identifier les e-mails malveillants avant qu'ils ne fassent de vous une victime.
  - Objet vague : aucune référence à un numéro de commande, à un produit, etc. Il peut être attrayant ou alarmiste et appelle à une action immédiate comme le changement de vos informations de connexion ou vos données personnelles, bancaires…
  - Grammaire : usage répétitif de « s'il vous plaît/SVP » dans le corps du message, tournures de phrases maladroites.

- Manque de personnalisation : la formule de salutation indique seulement « salut » ou « hi/hello », ce qui est étrange pour un e-mail aussi spécifique (il ne s'agit pas d'un envoi en masse).
- Manque de détails : formulation très simple, aucun détail sur le produit ou le service, pas de référence à un contact précédent.
- Nom du fichier : le nom de la facture n'est pas spécifique à un projet ou à une société, il n'y a aucun détail.
- Signature incohérente : les informations dans la signature de l'e-mail ne concordent pas avec les informations sur l'expéditeur (nom et adresse e-mail)
- L'email vous invite à cliquer sur un lien hypertexte sans préciser clairement la destination de ce lien. Pour rappel, lorsque vous passez votre curseur sur le lien sans cliquer dessus, cela vous montrera l'adresse de destination.

En cas de doute, contactez le service informatique du Groupe par tous moyens mis à disposition et signaler tous les mails qui vous sembleraient suspects. Ils seront analysés et si nécessaire, remontés à la DSI du groupe pour être supprimés automatiquement sur l'ensemble des messageries du groupe.

Principe 9 : signalement des incidents

L'utilisateur doit être impliqué et vigilant. Chaque utilisateur signale au service compétent tout incident (vol, perte, intrusion, virus, piratage, etc.) affectant les ressources informatiques et de télécommunication du Groupe.

Exigence 9.1 : signalement des incidents

L'utilisateur doit signaler les événements lui paraissant suspects à ses contacts informatiques et/ou ses contacts RGPD et conformité.

Chaque utilisateur doit notamment signaler sans délai au service concerné toute anomalie qui lui permettrait notamment d'accéder à des ressources du Groupe auxquelles il ne devrait normalement pas accéder ainsi que toute perte ou vol d'équipements informatiques ou tout autre incident.

VI. Droit à la déconnexion

La loi 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels a créé un droit individuel à la déconnexion qui repose sur la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos, de congés ainsi que pendant l'ensemble des périodes de suspension du contrat de travail.

6.1 Les modalités du droit à la déconnexion

Les modalités du droit à la déconnexion sont les suivantes :

- absence d'obligation de rester connecté(s) pendant les temps de repos ou de suspension du contrat de travail (déjeuner, repos quotidien et hebdomadaire, congés payés, RTT, congés maladie, …),
- droit à une réponse différée hors temps de travail,
- droit à une réponse différée pendant le temps de travail.

Il est également recommandé à chacun de s'accorder des temps de déconnexion pendant le temps de travail, afin de mieux se concentrer sur certaines tâches : ne pas céder à l'instantanéité de la messagerie, gérer les priorités, se fixer des plages horaires pour répondre.

6.2 Lutte contre la surcharge de l'information

Afin d'éviter la surcharge informationnelle, il est recommandé à chacun de respecter l'objet et la finalité des moyens de communication mis à leur disposition, tant en termes de forme que de contenu.

En ce sens, outre le respect des règles de bonnes pratiques dans l'utilisation de la messagerie électronique susvisées, tout salarié veille également à limiter les envois en dehors des heures de travail et à privilégier le face à face ou le téléphone dans la mesure du possible.

Les managers ne contactent pas leurs équipes en dehors du temps de travail, à moins que la gravité, l'urgence, ou l'importance du sujet en cause, ne le justifie.

6.3 Sensibilisation et exemplarité des comportements de la direction et du management

L'affirmation nouvelle de ces règles d'usage et du droit à la déconnexion de tout un chacun sera diffusée auprès de l'ensemble des salariés.
Pour que ce droit soit efficace, chacun doit pouvoir prendre conscience de sa propre utilisation des outils numériques et doit respecter le nécessaire temps de repos de ses collègues, à commencer par la direction et le management qui s'assurent de l'exemplarité de leur comportement.

Les managers veillent, par ailleurs, à réaliser un travail d'organisation de manière à ce que la charge de travail soit compatible avec l'exercice du droit à la déconnexion, pour eux-mêmes et pour leurs équipes.
Cela consiste notamment à anticiper des délais réalistes pour les différents projets en définissant clairement des priorités en fonction de la charge, ou encore à optimiser les réunions. Elles sont planifiées dans le respect des horaires des différents sites sauf urgence ou activité spécifique, les heures de début et de fin sont respectées, l'efficacité est recherchée.

VII. Rappel de la législation et de la réglementation européennes et françaises.

Chaque utilisateur doit se conformer aux lois et réglementions en vigueur et, notamment, au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et à la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

7.1 Protection des Données Personnelles (PDP)

Depuis le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur.
Ce règlement européen, ayant pour objet une meilleure protection et structuration des traitements de données personnelles, impose à toute entreprise de plus de 250 salariés une conformité obligatoire permettant notamment :

- Une minimisation des données collectées,
- Une transparence dans le traitement des données personnelles,
- L'exercice pour tous citoyen et/ou résident européen de ses droits notamment de modification, rectification ou suppression relatif à ses données personnelles.

Aussi, le RGPD confie à un organisme de contrôle étatique le soin de vérifier, par le biais de campagnes aléatoires d'audit ou sur plaintes, le degré de conformité des entreprises visées par ces dispositions légales.

A défaut de conformité, l'organisme de contrôle étatique peut être amené à infliger, à l'entreprise en défaut, une amende pouvant atteindre 4% du chiffre d'affaire mondial annuel.

En France, l'organisme de contrôle de la conformité au RGPD est la Commission Nationale de l'Informatique et des Libertés (CNIL).

7.1.1 Traitements groupe

Des traitements de données personnelles automatisés et manuels sont effectués par Hutchinson dans chaque établissement. Hutchinson déclare les traitements suivants :

- Gestion des processus de recrutement – Modalités de conservation définies par la loi locale
- Gestion des processus de paye et SIRH – Modalités de conservation définies par la loi locale
- Gestion du personnel – Modalités de conservation définies par la loi locale
- Messagerie – lié à l'utilisation du service - Suppression 3 mois après un départ
- Contrôle Internet – Rapport quantitatif – Suppression 3 mois après l'enregistrement

7.1.2 Traitements sites

Les chefs d'établissement sont responsables du respect de la loi pour les systèmes d'information dans leur établissement.

VIII. Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

IX. Information des salariés

Conformément aux articles L.1321-4 et R.1321-1 à R.1321-6 du Code du travail, la présente Charte a été :

- soumise pour avis au Comité social et économique pour les matières relevant de sa compétence,
- communiquée en deux exemplaires, accompagnés de l'avis des représentants du personnel, à l'inspecteur du travail,
- déposée au secrétariat greffe du conseil de prud'hommes,
- affichée dans les locaux de l'entreprise sur le panneau réservé à cet effet, en annexe du règlement intérieur,
- communiquée individuellement à chaque salarié.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise.

Des opérations de communication internes sont organisées afin d'informer les salariés sur les pratiques d'utilisation des systèmes d'information.

X. Modalité de diffusion et d'entrée en vigueur

Ce document est publié sur l'intranet du groupe dans : Système d'information / Référentiel
La présente charte est applicable à compter de l'accomplissement des modalités fixées au point IX de la présente Charte. Elle annule et remplace celle précédemment en vigueur.