HeadMind Partners

Charte d'utilisation des systèmes d'information

du Groupe HeadMind Partners

Sommaire

Préambule

Les systèmes de communication, d'information et les services numériques sont de plus en plus interconnectés, la transformation numérique est à la fois signe de progrès et déclencheur de risques.

Les bénéfices ne sont plus à démontrer, cependant la fiabilité des services numériques sera assurée à la condition que les systèmes soient sécurisés et que les données soient protégées.

Afin que chacune des parties puisse exploiter au mieux ces technologies tout en s'assurant du bon fonctionnement, il est impératif de déterminer un juste équilibre entre l'utilisation de ces ressources et la protection des intérêts de l'entreprise.

Objet :

L'objet de la présente Charte est d'informer les utilisateurs des modalités d'utilisation et de contrôle des ressources informatiques du Groupe HeadMind Partners.

Ainsi la présente charte informatique définit :

- les règles d'utilisation de l'ensemble des outils des systèmes d'information du Cabinet HeadMind Partners ;
- les modalités des contrôles qui peuvent ou sont réalisés dans le cadre de l'utilisation des ressources, afin que chaque utilisateur en soit informé.

Elle fait l'objet d'une validation préalable du Comité Social et Economique. Elle est rédigée dans le respect des valeurs de discrétion, de déontologie et de réserve qui régissent Headmind Partners .

Champ d'application :

La charte s'applique à l'ensemble des utilisateurs ayant accès aux ressources informatiques du Groupe Headmind Partners.

L'accès aux systèmes d'information donne des droits, mais aussi des devoirs qui n'ont d'autre but que de préserver HeadMind Partners, ses utilisateurs et ses clients. Aussi, chaque utilisateur s'engage à avoir pris connaissance de la charte et à accepter les conditions qui y sont présentées.

On désignera sous le terme **« Utilisateur » ou « Collaborateur »** toute personne ayant accès, ou utilisant les ressources informatiques, accès Internet, la messagerie électronique, quel que soit son statut (CDI, CDD, Intérimaire, stagiaire, prestataire…) quel que soit son lieu d'accès, que l'entreprise soit propriétaire ou non des équipements utilisés pour accéder aux ressources.

Les **« ressources informatiques »** sont l'ensemble de moyens informatiques et de télécommunications, matériels ou logiciels, que l'entreprise met à disposition des Utilisateurs afin que ceux-ci puissent accomplir leurs tâches professionnelles. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (accès à l'Internet, réseaux de transmission voix ou données, téléphones fixes ou portables, télécopieurs, service de visio-conférence, etc.), les équipements de stockage de données (disques durs externes, clés USB, supports optiques tel que le DVD etc.), les données contenues sur les équipements précédemment cités, les moyens de protection des équipements précédemment cités (câble de sécurité, filtre de confidentialité, carte ou jeton d'authentification), les applications informatiques et autres logiciels font partie des ressources du système d'information du Groupe Headmind Partners.

On désignera par **« compte »** l'association d'un identifiant et d'un ou plusieurs facteurs d'authentification, constituant le système d'authentification aux ressources informatiques.

1. Les usages et règles de sécurité

1.1. Généralité sur les usages

Chaque Utilisateur doit adopter un **comportement responsable et professionnel lors de l'utilisation des services et des ressources informatiques** afin de ne pas perturber ou empêcher leur bon fonctionnement, ni entrainer un détournement des activités à des fins non professionnelles ou illégales.

Chaque Collaborateur s'engage à respecter vis-à-vis des ressources connectées mise à sa disposition par le Cabinet :

- Une utilisation loyale en prévenant et en s'abstenant de toute malveillance destinée à perturber ou porter atteinte aux intérêts de HeadMind Partners ;
- Une utilisation strictement professionnelle et conforme à la finalité du Cabinet ;
- Une utilisation rationnelle dans le cadre personnel ;
- Une restitution dans un état similaire à celui lors de la mise à disposition.

1.1.1 Usage à des fins professionnelles

Les ressources informatiques mises à la disposition des Collaborateurs ou Utilisateurs sont réservées à un usage professionnel, afin de réaliser les missions, tâches qui leurs sont confiées dans le cadre de l'exercice de leur fonction tout en respectant les dispositions légales et conventionnelles applicable dans le Cabinet et sur les missions.

1.1.2 Usage à des fins personnelles

Bien que l'utilisation d'internet ou de la messagerie électronique du Cabinet doit être faite dans un but professionnel, HeadMind Partners tolère l'envoi ou la réception de messages électroniques ou l'utilisation d'Internet à des fins personnelles dans le cadre des nécessités de la vie privée, à condition que cette pratique soit occasionnelle et raisonnable et qu'elle soit conforme à la législation en vigueur et qu'elle ne porte pas atteinte à l'image du Cabinet.

Tout fichier, répertoire de fichier, e-mail personnel envoyé par le biais de la messagerie ou d'Internet doit être marqué en objet de la mention « personnel » ou équivalent « privé », « perso ». En l'absence de l'une de ces mentions, les fichiers, répertoires ou messages électroniques sont présumés professionnels. Le Collaborateur s'engage à ce que le contenu de ce type d'e-mail, fichier, répertoire corresponde effectivement à des éléments ne concernant pas directement ou indirectement HeadMind Partners.

En cas d'utilisation des ressources du Cabinet à des fins personnelles, il est demandé aux Collaborateurs de retirer la signature professionnelle automatique et de supprimer toute référence au Cabinet (en-tête, pied de page, etc.).

Tout e-mail stocké ou envoyé, ayant pour objet la mention « personnel », est protégé par le secret de la correspondance.

L'usage personnel des moyens informatiques fournis par le Cabinet pour répondre à des besoins réglementaires spécifiques est interdit.

1.1.3 Usage responsable

1.1.3.1 Imputabilité

Chaque Utilisateur s'engage à utiliser les ressources informatiques du Cabinet de manière responsable.

Le Collaborateur ou Utilisateur est responsable de toute action menée sous son identité :

- De toute connexion à Internet, à la messagerie électronique et toutes applications du Cabinet effectuée à l'aide de son identifiant et de son mot de passe, tant que son compte est actif ;
- De l'utilisation des ressources obtenues sur Internet et sur la messagerie électronique effectuée à l'aide de son identifiant et de son mot de passe, tant que son compte est actif.

Le Collaborateur doit signaler aux équipes de la Direction du Système d'Information (DSI) ou à l'équipe de la Sécurité du Système d'Information (SSI) toute suspicion d'utilisation frauduleuse de son compte. La responsabilité personnelle du Collaborateur ou Utilisateur pourra en effet être engagée en cas d'utilisation frauduleuse ou illégale des ressources informatiques du Cabinet réalisée avec son compte ou, le cas échéant, avec un équipement qui lui aura été affecté en propre.

1.1.3.2 Responsabilité du Collaborateur

Le Collaborateur dispose de comptes personnels incessibles. Il est alors l'unique responsable de leurs utilisations sur l'ensemble des moyens informatiques mis à sa disposition

Ainsi, si chaque Collaborateur du Cabinet a la possibilité de communiquer librement dans le Cabinet, il doit le faire sans abus, c'est-à-dire d'une part dans les limites habituelles des nécessités professionnelles, et d'autre part en respectant l'obligation de discrétion et de secret professionnel résultant de son contrat de travail et de la nature de ses fonctions.

Le Collaborateur doit se restreindre à son périmètre d'habilitation. Le Collaborateur ne doit pas contourner ou de tenter de contourner les restrictions d'accès. Le Collaborateur doit utiliser les applications conformément aux principes d'utilisation communiqués dans les politiques et procédures.

Tout Collaborateur est tenu d'assurer la protection des données métier et à caractère personnel qu'il traite dans le cadre de ses fonctions. Le Collaborateur ne doit pas conserver ces données au-delà de la durée nécessaire au traitement.

Le Collaborateur doit être vigilant au bon fonctionnement des équipements qui lui sont mis à disposition au regard du SI et ceux en complément des processus de contrôle automatisés mis en place par la DSI.

Lorsque qu'un dysfonctionnement du SI est constaté, chaque Collaborateur a la responsabilité de le signaler à la DSI par une demande électronique à travers les outils mis à sa disposition.

Ainsi chaque Utilisateur doit :

- Maintenir en bon état les ressources informatiques qui lui sont prêtées dans l'exercice de ses fonctions ;
- Restituer l'ensemble des ressources informatiques dès lors qu'il y a rupture de la relation contractuelle pour quelque cause que ce soit ;

- Respecter les lois et règlements en vigueur.

1.1.4 Usage interdit

Sans que cette liste soit limitative, il est strictement interdit de :

- Télécharger sur Internet pour un usage personnel puis de stocker et distribuer des images, des photos, des vidéos ou des fichiers musicaux ainsi que des logiciels ;
- Visionner, télécharger, stocker, distribuer des images portant atteinte au respect de la personne humaine (pornographie, racisme, etc.), images ou textes à caractère diffamatoire ou illicite, portant ainsi atteinte à l'image de marque interne ou externe du Cabinet ;
- S'inscrire à partir de son poste de travail à un forum de discussion sur Internet (sauf accord express de l'employeur pour raisons professionnelles), participer à des jeux ou loteries en ligne, créer des pages Web personnalisées de tout type, des sites blogs ;
- Créer un site à partir de son poste de travail à des fins étrangères à ses attributions ;
- Utiliser les ressources internes du Cabinet (intranet, messagerie) à des fins de diffamation, d'injure, de harcèlement, de menace ;
- Utiliser les ressources internes pour diffuser des informations confidentielles relatives au Cabinet, à ses membres et à ses partenaires commerciaux, sauf dans le cadre strict de la réglementation et de la conduite des affaires du Cabinet. Ainsi que tous actes susceptibles d'engager la responsabilité civile et pénale de son auteur ou de l'employeur ;
- Contourner, altérer ou supprimer les règles et dispositifs mis en œuvre par le Cabinet pour s'assurer de l'usage responsable des ressources informatiques de la société ;
- Manipuler de l'information Diffusion Restreinte (DR) sur un système d'information non homologué DR ;
- Porter atteinte aux intérêts légitimes du Cabinet.

Il est également demandé à chaque Collaborateur de faire preuve de la plus grande correction à l'égard des interlocuteurs quels qu'ils soient (clients, Collaborateurs, autres personnes extérieures, etc.) dans les échanges écrits et par téléphone. Le Collaborateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen écrit.

1.2. Règles de sécurité dans les usages

1.2.1 Règles générales de sécurité et bon fonctionnement

Tout Collaborateur, en cas d'absence temporaire, est prié d'appliquer les bonnes pratiques de sécurité des terminaux mobiles tel que : la sauvegarde des fichiers en cours de travail, la sécurisation du poste par un câble antivol et le verrouillage de la session.

Il est aussi demandé d'appliquer les bonnes pratiques de bureau propre et de détruire les documents papier avec les broyeurs mis à disposition afin de maintenir une sécurisation et une confidentialité de l'environnement de travail optimales.

Le Collaborateur doit veiller à ne laisser aucun document à la portée d'autrui et sans surveillance sur les lieux de travail, imprimantes ou tout autres matériels mis à sa disposition.

En cas de départ du Collaborateur, démission, licenciement, rupture de période d'essai, son compte professionnel sera désactivé dès son départ physique du Cabinet et sera ensuite supprimé dans un délai de quatre mois à compter du jour de départ du Cabinet.

HeadMind Partners appliquera le processus décrit dans sa politique de Gestion Des Habilitations pour supprimer et modifier les droits d'accès à l'intranet, ainsi qu'aux applications métiers du compte d'un Collaborateur en cas de départ ou changement de fonction en interne.

Il est interdit à tous les Collaborateurs de connecter tout terminal portable personnel (Smartphone, ordinateur portable) au réseau informatique du Cabinet, hors wifi-guest, et ce quel que soit le moyen utilisé. La DSI ne réalise pas de support sur ces terminaux en cas de dysfonctionnement et le Collaborateur pourra être tenu responsable en cas d'incident sur le système d'information HeadMind Partners.

1.2.2 Authentification

L'authentification d'un Collaborateur ou Utilisateur se fait à travers un compte utilisateur associé à 'un ou plusieurs facteurs d'authentification dispositifs indispensables pour assurer la protection des ressources informatiques du Cabinet et l'imputabilité des actions aux Collaborateurs ou Utilisateurs.

Ainsi, le Cabinet fournit à chaque Collaborateur les moyens d'authentification qui lui permettent d'utiliser les outils informatiques : ordinateurs, réseaux, messagerie et autres applications du Cabinet.

Cette identification permet l'attribution de droits et privilèges propres à chaque Utilisateur sur les ressources du système dont il a besoin dans l'exercice de sa mission.

L'usage de ces moyens d'authentification doit rester confidentiel pour réduire les risques d'usurpation d'identité. Ces moyens sont strictement personnels. Le Collaborateur ne doit en aucun cas communiquer ses informations personnelles à autrui. Il ne doit également pas, non plus, tenter d'utiliser le compte d'un autre Collaborateur.

Les moyens d'authentification associés à un compte sont propres au Collaborateur détenteur. Ils devront être alignés avec les spécifications exprimées dans la Politique de Mot de Passe en place afin d'en garantir sa sécurité et celle du système d'information de HeadMind Partners. Chaque Collaborateur est responsable de l'utilisation qui est faite de ses moyens d'authentification. Le Collaborateur ou Utilisateur doit être attentif aux alertes et délais.

Pour toute information relative aux moyens d'authentification, se reporter à la procédure figurant sur l'intranet du Cabinet, ou sur les politiques en vigueur sur le système d'information Diffusion Restreinte.

Par ailleurs, en vue de s'assurer de l'identité de l'Utilisateur, le Cabinet a et peut requérir l'emploi de support types cartes (pour les imprimantes) complété d'un code secret pour accéder à des ressources informatiques. Mais aussi des codes et des processus particuliers pour se connecter au système d'information du Cabinet depuis l'extérieur.

1.2.3 Confidentialité

L'obligation de confidentialité a pour but de protéger les intérêts du Cabinet, par conséquent elle s'oppose à la communication d'informations ou de données de quelque nature que ce soit que le Collaborateur ou Utilisateur aurait connaissance du fait de ses habilitations ou à l'occasion de ses activités dont il a la responsabilité et dont la divulgation aurait pour effet de nuire aux intérêts du Cabinet.

Chaque Collaborateur a un devoir strict de confidentialité à l'égard des informations professionnelles auxquelles il a accès au Cabinet et doit se conformer aux règles établies dans la politique de classification des données.

Les données professionnelles auxquelles les Collaborateurs ont accès dans le cadre de leurs fonctions sont la propriété exclusive de HeadMind Partners et de ses filiales.

Conformément à ces règles de confidentialité, le Collaborateur a également un devoir strict de confidentialité à l'égard des informations auxquelles il pourrait avoir accès au sein des sociétés prestataires ou clientes auprès desquelles il pourra être amené à intervenir dans le cadre de ses missions. Communications orales, e-mails, réseaux sociaux, etc. doivent ainsi être strictement utilisées dans le respect de cette confidentialité.

L'utilisation d'un assistant personnel (smartphone, tablette, etc.) incluant les mêmes fonctionnalités est soumise aux règles de la présente charte. Les possesseurs d'assistants personnels ont notamment un devoir strict de confidentialité à l'égard des informations professionnelles transitant dessus.

Il est rappelé que le fait de copier et s'approprier des données confidentielles appartenant au Cabinet constitue une violation du secret des affaires. En cas de manquement, le Collaborateur s'exposerait à une sanction et/ou des poursuites civiles ou pénales.

1.2.4 Archivage des données et conservation

Les fichiers, messages et données électroniques manipuler par les Collaborateurs ou les Utilisateurs font partie intégrante des biens immatériels du Cabinet. La conservation de ces biens est primordiale pour sécuriser la continuité de l'activité du Cabinet, son savoir-faire, la propriété intellectuelle de ses métiers et être en capacité de répondre à ses obligations légales.

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et d'un dispositif miroir destiné à doubler le système en cas de défaillance.

1.3. Usages des moyens mis à disposition

1.3.1 Messagerie électronique

L'ensemble des Collaborateurs de HeadMind Partners dispose, pour l'exercice de leur activité professionnelle, d'une boîte au lettre électronique individuelle (messagerie) leur permettant de communiquer, par e-mail, au sein du Cabinet ou vers l'extérieur ainsi qu'une messagerie instantanée. Les modalités d'accès à la messagerie et à la messagerie instantanée sont identiques aux modalités d'accès à l'intranet et à Internet.

Comme le courrier ordinaire (papier), la messagerie électronique peut engager le Cabinet, notamment auprès des tiers. L'Utilisateur doit faire preuve de précaution dans son utilisation notamment :

- Respecter les règles de bon usage : s'identifier clairement (nom, fonction, entité), être bienséant avec ses interlocuteurs, être attentif aux destinataires, préciser l'objet et de manière générale s'abstenir de tout contenu contraire à l'ordre moral (diffamation, incitation à la violence, à la haine raciale, injures etc.) ou illégal.
- Respecter les règles de protection et de classification des messages en vigueur dans le Cabinet (cf. Confidentialité 1.2.3).
- Ne pas utiliser une messagerie privée (internet) pour les échanges professionnels.
- Préciser de la mention « personnel » pour tout message à caractère personnel.
- Envoyer des pièces jointes sur des adresses emails non professionnelles, en cas d'envoi un message d'avertissement sera adressé au Collaborateur ou Utilisateur.

Ces éléments d'usage s'appliquent à la messagerie électronique classique (email) mais aussi à tout autre moyen d'échange électronique type sms (Short Message Service), messagerie instantanée (tchat) etc.

Enfin la messagerie est un outil d'information fortement ciblée par les pirates et les personnes malveillantes :

- Divulgation d'information par interception des e-mails ou envoi non intentionnel à une tierce personne ;
- Transmission de virus par pièces jointes.

Dès lors, la messagerie est protégée par un pare-feu ayant pour finalité la protection contre les attaques informatiques et les messages indésirables.

Certains fichiers peuvent contenir des virus donc certaines pièces jointes des mails sont bloquées aussi bien en émission qu'en réception. Des exemples d'extension non permises : MP3, EXE, BAT, etc.

Dans le cadre de la boîte aux lettres de la messagerie, trois seuils limites ont été définis :

- Limite 1 : message d'alerte à 1,9 Go ;
- Limite 2 : blocage de l'envoi à 2 Go ;
- Limite 3 : blocage de l'envoi/réception à 2,1 Go.

Une notification par e-mail est envoyée au Collaborateur ou Utilisateur chaque fois qu'une des limites est atteinte.

1.3.2 Internet

L'ensemble des Collaborateurs de HeadMind Partners travaillant au siège a la possibilité de se connecter de façon permanente à Internet depuis le Cabinet, à partir de son poste de travail, sauf sur les sites interdits pour des raisons légales, de sécurité ou de contenu explicite.

Si le Collaborateur souhaite accéder à un site bloqué qu'il pense légitime, il pourra et devra informer la DSI en justifiant sa demande.

Il existe une restriction sur les téléchargements. Le Collaborateur ou Utilisateur qui souhaite télécharger plus de 25 Mo doit faire une demande à la DSI. Cette mesure vise à prévenir d'une éventuelle saturation de la bande passante internet. Le téléchargement de fichier type MP3, EXE, BAT, etc. n'est pas autorisée.

1.3.3 Réseaux sociaux

Les réseaux sociaux sont devenus indispensables dans la valorisation des activités du Cabinet. Ils sont devenus des outils de communication internes et externes.

Ainsi, tout Collaborateur s'engage à :

- Etre réservé et attentif quand il écrit sur les réseaux sociaux car il engage sa responsabilité dans les contenus qu'il met en ligne ainsi ne pas publier d'information:
    - à caractère confidentiel ;
    - relative à un collègue sans son accord explicite ;
    - portant atteinte à l'image du Cabinet ;
    - en usurpant l'identité d'un tiers.
- Ne pas créer de compte ou animer un compte au nom du Cabinet sans y avoir été préalablement autorisé par la Direction.
- Respecter les réglementations relatives à la propriété intellectuelle en cas d'utilisation de photo, marque, logo, vidéo etc., en demandant préalablement l'autorisation au titulaire des droits, ou demandant l'autorisation des personnes figurant sur des photos ou autre dans le cadre du respect du droit à l'image.
- Respecter les points de vue de ses lecteurs, en s'abstenant de toute publication illicite notamment injurieuse, raciste, discriminatoire, diffamatoire etc., en riposte.

1.3.4 Poste de travail et périphériques

Le poste de travail mis à disposition du Collaborateur dans l'exercice de sa mission, lui permet d'avoir accès au réseau du Cabinet et par conséquent à un nombre important de données conservées sur le poste de travail, la GED interne, les applications informatiques…

Dès lors, le Cabinet protège son patrimoine immatériel à travers une politique de sécurité forte moyennant des dispositifs :

- de protection :
    - au bout de 8 minutes d'inactivité , la session est automatiquement verrouillée pour prévenir d'une utilisation frauduleuse,
    - Lorsque la session est verrouillée, le nom de l'Utilisateur connecté n'est pas apparent,
- de surveillance automatisés de type pare-feu, antivirus etc.,
- des actions manuelles des administrateurs informatiques.

Au-delà des mesures prises par le Cabinet, le Collaborateur ou Utilisateur doit **:**

- Sécuriser la session en verrouillant l'accès au poste de travail, sans attendre la mise en veille automatique, dès lors qu'il s'éloigne de son poste ;
- Sécuriser le poste de travail portable, avec le câble antivol fourni ;
- Utiliser les outils de sauvegarde (clé usb, disque dur externe…) mis à disposition par le Cabinet et/ou après autorisation de la DSI, qui se sera assuré de l'absence de dangerosité (logiciel malveillant, virus etc.) ;

- Ne pas désinstaller, modifier ou désactiver un logiciel standard notamment l'antivirus.

En outre, il ne doit pas :

- Installer de logiciel sans avoir obtenu l'autorisation préalablement ;
- Connecter de poste de travail externe au réseau du Cabinet, en dehors des moyens fournis par le Cabinet pour y parvenir (authentification renforcée) ;
- Connecter le poste de travail interne à un réseau externe, en dehors des moyens fournis par le Cabinet.

Chaque poste informatique est protégé contre toute installation de logiciels. Toute demande d'installation, de droit d'administration et d'accès exceptionnel (sortant du cadre précis métier/fonctionnel du Collaborateur) devra passer par une demande électronique aux équipes de la DSI et sera soumise à validation managériale.

1.3.5 Outils de mobilité

L'ensemble du personnel de HeadMind Partners dispose d'un téléphone mobile professionnel et d'un forfait qui y est associé.

Outre le téléphone mobile, certains Collaborateurs peuvent se voir attribuer dans l'exercice de leur fonction d'autres outils de mobilité de type : ordinateur portable, une tablette, dispositif de connexion en accès distant, etc.

Les règles qui s'appliquent au poste de travail classique s'appliquent également aux outils de mobilité et de manière globale à l'usage professionnel.

Outre les principes déjà énumérés, l'Utilisateur des outils de mobilité doit :

- Se montrer attentif et précautionneux lors des déplacements en prenant soin de ne pas laisser son matériel sans surveillance et accessible à des tiers ;
- Déclarer la disparition aussi rapidement que possible afin de couper les accès au réseau interne et diligenter les procédures adéquates (déclaration de perte, vol etc.) ;
- Ne pas prêter son matériel à un tiers, y compris un Collaborateur de la société car l'attribution est nominative et incessible.

Mesures spécifiques à l'ordinateur portable :

- Veiller à stocker régulièrement les données professionnelles (réseau, Cobalt, Filao) ;
- Ne pas installer d'application qui n'a pas été autorisée ;
- Ne pas se connecter à des réseaux wifi ouverts et/ou non protégés qui peuvent intercepter des messages, informations ;
- Se connecter régulièrement au réseau afin de permettre les mises à jour régulière des logiciels et anti-virus ;
- Au bureau, l'ordinateur portable doit toujours être attaché à l'aide d'un câble antivol ;
- Si le Collaborateur l'emporte avec lui, il doit porter une attention et surveillance particulière ;
- Les supports de stockage externe ne sont ni des supports de sauvegarde, ni d'archivage.

Mesures spécifiques à l'impression :

Au sein du Cabinet, les impressions sont sécurisées.

Le Collaborateur et ou Utilisateur reçoit, lors de la première impression, par email un code à 5 chiffres. Ce code permet des impressions sécurisées.

Mesures spécifiques au clé USB :

Un outil de cryptage pour clé USB est mis à disposition des Collaborateurs. Il sert à sécuriser les dossiers professionnels se trouvant sur la clé USB de l'Utilisateur, à l'aide d'un mot de passe.

Mesures spécifiques à la téléphonie :

- Ne pas installer d'application mobile qui n'a pas été autorisée ;
- Ne pas se connecter à des réseaux wifi ouverts et/ou non protégés qui peuvent intercepter des messages, informations.

1.3.6 Accès aux systèmes d'information métier

L'accès aux applications métiers est conditionné à l'appartenance du Collaborateur aux métiers concernés (recrutement, commercial, gestion des carrières, etc.). Le Collaborateur accède à ces applications par l'intermédiaire de son compte personnel. Cet accès peut évoluer dans le temps en fonction de son affectation.

L'accès aux systèmes d'information est, de plus basé, sur le principe du moindre privilège et du besoin d'en connaître.

Chaque poste informatique est protégé contre toute installation de logiciels. Toute demande d'installation, de droit d'administration et d'accès exceptionnel (sortant du cadre précis métier/fonctionnel du Collaborateur) devra passer par une demande électronique sur le portail GLPI et sera soumise à validation managériale.

Au-delà des exigences déjà évoquées, le Collaborateur ou Utilisateur s'adapte et applique les dispositions spécifiques liées à ces applications métiers.

1.3.7 Intranet

Chaque Collaborateur bénéficie au moment de son arrivée dans le Cabinet d'un compte lui permettant d'accéder à l'intranet et aux ressources informatiques à partir de son poste de travail, chez le client, ou depuis son domicile lorsque les spécificités de sa mission ne lui permettent pas une connexion chez le client.

L'intranet permet au Collaborateur :

- D'avoir de l'actualité sur le Cabinet ;
- D'accéder aux espaces des communautés internes ;
- Lancer des Workflow (demande de congés, déclaration des temps, des frais…) ;
- Coopter ;
- Retrouver des raccourcis aux applications métiers (Sage pour la déclaration des temps et des frais ;

- Recevoir des notifications.

2. Mesures de contrôle

Les Collaborateurs sont informés que les dispositifs mis en place par le Cabinet pour contrôler les accès à Internet et à la messagerie électronique permettent d'enregistrer :

- La trace de l'ensemble des sites Web consultés ;
- La trace des connexions aux différents services exposés par les systèmes d'Information ;
- Des informations échangées ;
- Des messages émis et reçus ;
- Des téléchargements de fichiers effectués.

Ces outils peuvent être utilisés à des fins de contrôle, de façon inopinée ou en cas d'incidence ou de malveillance. De plus, le Cabinet se réserve le droit de bloquer tout fichier susceptible de contenir des virus actifs.

Tant par mesure de sécurité (virus, intrusion) que par nécessité du Cabinet de se prémunir contre un risque de « pillage » de fichiers confidentiels, les e-mails envoyés par les Collaborateurs auxquels sont joints des fichiers attachés sont réputés être des e-mails professionnels, qu'ils soient ou non pourvus de la mention « personnel ». Ils peuvent, à ce titre, être consultés de manière tout à fait exceptionnelle, lorsque l'employeur soupçonne un comportement ou des actes délictueux.

Les postes de travail sont aussi protégés par un anti malware se mettant à jour. Le Collaborateur doit s'assurer de sa bonne mise à jour que ce dernier soit au siège de la société ou à l'extérieur.

Le Cabinet a la possibilité, en cas d'absence prolongée d'un Collaborateur (arrêt maladie, congés payés, RTT, mise à pied, etc.) d'accéder à sa messagerie électronique pour consulter les e-mails reçus, avec ou sans fichier attaché, et ce dans un souci de continuité de l'activité. Dans la mesure où ceux-ci sont marqués de la mention « personnel » et qu'ils ne contiennent pas de fichier attaché, le Cabinet s'interdit de les consulter.

2.1. Limitation dans l'utilisation des ressources

Le Cabinet se réserve la possibilité, à des fins d'audit, de statistiques ou de diagnostic d'activité, de vérifier les connexions ou tentatives de connexion de chaque Collaborateur aux services fournis par les systèmes d'Information, à Internet, , de contrôler les caractéristiques techniques des e-mails (taille du message, expéditeur, pièces jointes, etc.) ainsi que leur contenu, lorsque ceux-ci ne sont pas marqués « personnel ».

Les administrateurs du SI disposent de moyens de contrôle mis légalement à leur disposition, leur permettant une surveillance et une traçabilité des fichiers et e-mails transmis à l'extérieur du Cabinet. Ils sont en droit d'établir des procédures de surveillance de toutes les tâches effectuées sur les différents systèmes.
Les données permettant d'identifier le poste du Collaborateur sont conservées pendant une durée de deux mois.

Les administrateurs du système peuvent se réserver la possibilité d'accéder, à des fins de diagnostic technique, aux informations contenues sur chaque poste de travail, même « privatives », dans les cas où cette action est rendue nécessaire au bon fonctionnement général du système informatique du Cabinet. Dans ce cas, la personne habilitée s'engage à préserver la confidentialité des informations personnelles dont elle aurait eu connaissance.

2.1.1 Dispositif de blocage ou limitant l'emploi des ressources

A titre illustratif, il peut être question de :

- Bloquer des sites transgressant les principes d'usage responsable (cf.1.1.3) ;
- Bloquer la sortie hors du réseau du Cabinet de documents confidentiels ;
- Bloquer l'installation de logiciel sur le matériel du Cabinet ;
- Limiter les accès à internet ;
- Toutes mesures de blocage nécessaire à la protection des ressources informatiques et des intérêts légitimes du Cabinet.

2.1.2 Dispositif automatique de surveillance

Le Cabinet peut être amené à mettre en œuvre un dispositif de surveillance des ressources informatiques. Ces mesures font l'objet lorsque cela était nécessaire de déclaration auprès de la CNIL et de consultation des Instances Représentatives du Personnel. Le personnel est également informé de la mise en place de ces dispositifs de surveillance.

2.1.3 Déclaration des incidents de sécurité

Le Collaborateur ou Utilisateur doit informer la DSI ou le Responsable Sécurité SI (RSSI) de tout dysfonctionnement, anomalie ou incident susceptible de compromettre, bloquer le fonctionnement normal du système d'information nécessaire à la continuité de l'activité du Cabinet, qu'il détecte à l'occasion de l'utilisation des ressources.

2.2. Les mesures de contrôles automatisées

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien interne que distant. Il vérifie aussi le trafic entrant constitué de la messagerie électronique, l'échange de fichiers, et la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- des connexions aux différents services exposés par les systèmes d'Information ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe *(et éventuellement texte du message)*.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes *(complétez si nécessaire)*.

Les mesures de surveillance et de contrôle mis en place par le Cabinet visent à :

- Protéger les ressources informatiques des actes malveillants, illicites ;
- S'assurer de l'intégrité et disponibilités des ressources informatiques ;
- Garantir la sauvegarde des données et de l'activité de l'entreprise ;
- Garantir la confidentialité des données ;
- Répondre aux exigence légales.

Ces mesures de contrôle sont gérées par la DSI, les restitutions sont faites conformément aux dispositions légales ou procédures internes.

2.2.1 Contrôle des moyens de communication électronique

Le Collaborateur et/ou Utilisateur est informé que les outils de communication électroniques font l'objet de recueille d'informations et de contrôle notamment relatifs à l'identifiant, l'émetteur, nombre, volumétrie, fréquence d'envoi ou de réception des messages, présence de pièces jointes (volume), classification (privée/ Professionnelle)

Les données collectées sont conservées pendant 1 an et supprimées au-delà.

2.2.2 Contrôle de l'usage d'internet

Dans l'hypothèse la plus courante, les contrôles portent sur :

- les durées des connexions ;
- les sites les plus visités ;
- la volumétrie ;
- l'identité du Collaborateur ou Utilisateur ;
- adresses IP etc.

Ce contrôle permet de veiller aux potentielles attaques, par corrélation mais également d'être en mesure de réguler et d'adapter l'offre internet aux besoins du Cabinet.

Le Cabinet bloque automatiquement l'accès aux sites internet illicites ou contraire à l'usage raisonnable (jeux vidéo, jeux d'argents etc.).

Les données collectées sont conservées pendant 1 an et supprimées au-delà.

2.2.3 Contrôle des usages des mobiles

Les contrôles portent sur :

- la volumétrie des consommations ;
- l'identité du Collaborateur ou Utilisateur : émetteur (numéro de téléphone) et destinataire (relevés des appels). En cas de doute d'activité malveillante ou anormale, une analyse détaillée des communications peut être demandée. En cas d'utilisation professionnelle et privée le Collaborateur sera informé de la procédure afin de garantir la protection des données privées le concernant.

Les données collectées sont conservées pendant 1 an et supprimées au-delà.

2.2.4 Contrôle des connexions aux ressources IT

Les contrôles portent sur les données de connexions relatives à l'ensemble des accès aux ressources informatiques du Cabinet depuis un équipement mis à disposition ou autorisé par le Cabinet, quel que soit sa localisation. Les données concernées sont :

- les identifiants du matériel ;
- les identifiants des Utilisateurs ;
- les identifiants des ressources informatiques et des données ;
- la nature des données mais aussi date et volume des flux de connexion.

Cette collecte et sauvegarde est réalisée par la DSI afin de garantir la maintenance des infrastructures et de prévenir des incidents de sécurité par la détection d'anomalie évocateur d'actes de malveillance ou de dysfonctionnement (présence par exemple de virus, usurpation d'identité, logiciels malveillants etc.).

Les données collectées sont conservées pendant 1 an et supprimées au-delà.

2.2.5 Contrôle des systèmes d'information métier

Les contrôles portent sur :

- les données de connexions : identifiant, code de connexion etc.
- la volumétrie des consommations ;
- l'identité du Collaborateur ou Utilisateur.

En cas de traitement de données à caractère personnel, une information préalable est faite au Collaborateur.

2.3. Mesures de contrôle manuel

En cas de suspicion d'anomalie, de dysfonctionnement, d'acte malveillant, la Direction se réserve le droit d'autoriser un contrôle manuel des ressources informatiques afin d'identifier le fait anormal, fautif ainsi que l'auteur.

2.4. Accès aux données du Collaborateur

La procédure varie en fonction de la nature des données professionnelles ou personnelles mais aussi selon que les équipements appartiennent au Cabinet ou à l'Utilisateur.

2.4.1 Accès aux données professionnelles

La Direction, les responsables hiérarchiques ou la DSI, peuvent, sous certaines conditions, avoir aux données professionnelles notamment afin d'assurer la continuité de l'activité, en cas d'absence du Collaborateur ou pour un motif touchant à la sécurité du Cabinet.

2.4.2 Accès aux données personnelles

Les messages électroniques, répertoires ou fichiers identifiés comme personnels ne sont pas librement accessibles par la direction, les responsables hiérarchiques ou la DSI.

L'accès à ces documents doit se faire en présence de l'Utilisateur, en cas d'impossibilité de présence, il doit être préalablement informé.

Ces conditions ne sont pas requises en cas de danger économique ou menace terroriste, qui impactent le Cabinet et qui nécessite la prise de connaissance des données personnelles. A l'issue des investigations, l'Utilisateur sera informé.

3. Protection, gestion et respect des données

Les informations et les données relatives aux Collaborateurs, aux clients, aux partenaires et aux activités du Cabinet constituent son patrimoine.

Pour assurer sa sécurité, HeadMind Partners s'est muni d'une politique de sécurité pour son système d'information (PSSI) et d'une politique de gestion des données à caractère personnel. Le Cabinet a également sa propre classification des données et une procédure à suivre en cas de violation de données à caractère personnel. Tout Collaborateur s'engage à respecter lesdites politiques et procédures ci-avant énoncées.

3.1. Cadre juridique

HeadMind Partners s'engage à respecter les législations applicables au traitement des données ainsi qu'à leur utilisation, notamment le règlement n°2016/679 dit Règlement Général de la Protection des Données (RGPD).

La législation française en vigueur, en particulier les dispositions concernant le domaine de la sécurité informatique, doivent être respectées :

- La loi du 6 janvier 1978 dite « Informatique et libertés » ;
- Le règlement n°2016/679 dit Règlement Général de la Protection des Données (RGPD)
- La législation relative à la fraude informatique, articles 323-1 à 323-7 du nouveau code pénal ;
- La législation relative à la propriété intellectuelle ;
- La législation applicable en matière de cryptologie ;
- L'article 8 de la Convention européenne des droits de l'homme ;
- L'instruction Interministérielle 901 relative à la Protection des Systèmes d'Informations Sensibles ;
- L'article 9 du Code civil.

Tout Collaborateur ou Utilisateur doit respecter les dispositions législatives et réglementaires relatives à l'utilisation des technologies de l'information et de la communication.

Celles-ci prévoient en particulier les mesures interdisant :

- L'atteinte à la vie privée (i.e. opinions politiques, religieuses, philosophiques, aux origines ethniques, à la vie sexuelle ou à la santé des personnes) ;
- Les actes de violence écrite ou verbale ou contraire aux règles éthiques ou aux bonnes mœurs, notamment :
    - La diffamation et l'injure,
    - Le révisionnisme et l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité,

  - L'incitation aux crimes et délits (i.e. l'incitation au suicide, à la haine ou à la violence),
  - L'atteinte aux mineurs (i.e. exposition à des messages à caractère violent, pornographique ou pédopornographique),
  - L'incitation à la consommation de substances interdites ;
- La fraude informatique, incluant des actes tels que :
  - L'accès ou le maintien frauduleux dans un système de traitement automatisé de données,
  - La falsification, la modification, la suppression et l'introduction d'information avec l'intention de nuire ;
- La violation du secret professionnel, des affaires, des enquêtes et de l'instruction ;
- La violation de la propriété intellectuelle et du droit à l'image ;
- Le non-respect de la réglementation relative à la protection des données à caractère personnel ;
- Le non-respect de la réglementation liée à la protection de l'information Diffusion Restreinte

3.2. Engagement de l'Utilisateur

Chaque Collaborateur ou Utilisateur s'engage :

- à ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions ;
- à ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions ;
- à empêcher que les données ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations ;
- à ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses fonctions ;
- à prendre toutes les mesures conformes à l'état de l'art et aux règles internes dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- à prendre toutes précautions conformes à l'état de l'art et aux règles internes pour préserver la sécurité physique et logique de ces données ;
- à s'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés du Cabinet seront utilisés pour transférer ces données après accord écrit préalable des clients ou partenaires s'agissant du transfert de leurs données ;
- en cas de cessation de ses fonctions, à restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

3.3. Droit à l'information des Utilisateurs

Conformément au règlement n°2016/679 dit Règlement Général de la Protection des Données (RGPD), le Collaborateur dispose d'un droit d'accès, de rectification, d'opposition et de suppression des informations le concernant.
Pour ce faire, le Collaborateur adressera une demande écrite au Délégué à la Protection des Données (DPD), qui s'engage à lui répondre dans le mois qui suit la réception de la demande écrite.

3.4. Propriété intellectuelle et artistique / Logiciels

Il est strictement interdit au Collaborateur ou Utilisateur d'utiliser, de reproduire et plus généralement d'exploiter des œuvres protégées par le droit d'auteur ou un droit privatif sans l'autorisation du Cabinet ou du titulaire des droits et notamment des bases de données, des textes, des images, de la musique ou de la vidéo.

Il est strictement interdit au Collaborateur ou Utilisateur d'employer des logiciels pour lesquels le Cabinet ne dispose pas de droit de licence. Il est strictement interdit au Collaborateur ou Utilisateur d'effectuer des copies de logiciels pour quelque usage que ce soit.

4. Sanctions

La présente charte a pour objet de prévoir les conditions d'usage des moyens informatiques mis à la disposition des Collaborateurs dans le cadre de leurs fonctions. Elle a également pour but d'informer le Collaborateur sur les principaux risques d'ordre juridique liés à l'utilisation des services Internet et de la messagerie électronique du Cabinet.

En effet, de très nombreuses dispositions légales et réglementaires, dont beaucoup comportent des dispositions pénales, sont susceptibles de s'appliquer. Le Collaborateur doit donc avoir conscience qu'une utilisation inappropriée ou irréfléchie des services Internet, de la messagerie électronique et des données professionnelles et personnelles du Cabinet qui lui sont confiée, est susceptible d'engager sa propre responsabilité pénale et civile.

Tout usage des moyens mis à la disposition des Collaborateurs à des fins non autorisées par la présente charte expose ces derniers à la restriction ou à la suspension sans préavis des accès du Collaborateur aux ressources informatiques ou toute autre mesure que le Cabinet jugera nécessaire et au risque de sanction que le Cabinet se réserve la possibilité d'engager en fonction de la gravité des abus constatés, et ce conformément à l'échelle des sanctions applicables dans le Cabinet et prévue dans le Règlement intérieur.

En outre, en cas de manquement aux règles de la présente charte, d'agissement frauduleux, fautif ou dommageable, mettant en danger le bon fonctionnement du Cabinet commis de son fait, HeadMind Partners se réserve le droit d'enclencher un processus disciplinaire à l'encontre du Collaborateur et verra sa responsabilité personnelle engagée tant sur un plan civil que pénal pour tout type de préjudice.

Dans le cas où la responsabilité de HeadMind Partners ou de l'une de ses filiales serait engagée, ces derniers pourront se retourner contre le Collaborateur ayant enfreint les présentes dispositions.

De part le caractère non exhaustif des règles de conduite la responsabilité du Collaborateur n'est alors pas limitée aux seules définies ci-dessus. Il appartient donc au Collaborateur d'évaluer sa situation et d'agir dans le respect du bon sens, de l'éthique et de la réputation du Cabinet, et toujours de manière à sauvegarder l'intégralité des ressources informatiques du Cabinet.

En cas de doute du Collaborateur lors de l'utilisation des moyens informatiques sur la conformité de ses agissements face au texte ou à l'esprit de la présente charte ("ce que je suis en train de faire ou ce que je m'apprête à faire est-il conforme à la charte informatique ?") celui-ci doit immédiatement faire part de celui-ci à son responsable hiérarchique.

Tout consultant en mission s'engage à prendre connaissance de la charte informatique de son client et, dans la mesure où elle contiendrait des clauses plus limitatives que celles de la présente charte, à s'y conformer.

5. Opposabilité de la charte

La présente charte constitue un additif au règlement intérieur, elle est communiquée individuellement, à tout Collaborateur ou Utilisateur, avec le règlement intérieur du Cabinet lors de l'entrée au sein du Cabinet HeadMind Partners ou avant toute première utilisation des ressources.

La prise de connaissance et l'acceptation des règles décrites dans la présente charte restent un préalable à toute utilisation des ressources IT du groupe HeadMind Partners.

À ce titre, tout manquement à l'une quelconque de ses dispositions pourra entrainer les sanctions disciplinaires prévues par le règlement intérieur.

L'Utilisateur est régulièrement tenu au courant de l'évolution des limites techniques des Systèmes d'Information et sur les menaces susceptibles de peser sur sa sécurité. La présente charte et l'ensemble des politiques, procédures et règles techniques sont disponibles sur l'intranet du Cabinet.

L'Utilisateur atteste avoir lu avec attention la présente charte.