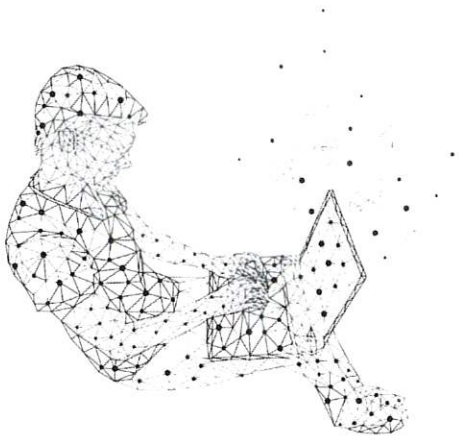
Cabinet de conseil en Data Protection

Charte d'utilisation des moyens d'informations



Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

Table des matières

Table des matières 2

1. Préambule et Organisation interne 4

2. Protection des Données Personnelles et droit applicable 5

1. Accès aux données à caractère personnel 5

2. Traitement de données à caractère personnel 6

3. Bonnes pratiques 7

1. Bien choisir ses mots de passe 7

2. Mettre à jour régulièrement vos logiciels 7

3. Bien connaitre ses utilisateurs et ses prestataires 7

4. Effectuer des sauvegardes régulières 7

5. Sécuriser l'accès Wi-Fi 8

6. Être aussi prudent avec son smartphone qu'avec son ordinateur 8

7. Protéger ses données lors de ses déplacements 8

8. Être prudent lors de l'utilisation de sa messagerie 9

9. Télécharger ses programmes sur les sites officiels des éditeurs 9

10. Être vigilant lors d'un paiement sur internet 10

11. Séparer les usages personnels des usages professionnels 10

12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique 11

4. Accès aux ressources informatiques 11

5. Règles d'utilisation et de sécurité 12

6. Règles de confidentialité 13

7. Respect de la législation concernant la propriété intellectuelle 13

8. Préservation de l'intégrité des systèmes informatiques 14

9. Usage des services internet 14

10. Droits et devoirs spécifiques des administrateurs systèmes et/ou réseaux 14

11. HADOPI 15

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

12. Infraction à ces règles 15

13. Télétravail..... 16

1. Accès à internet.....16

2. Mot de passe.....16

3. Sécurisation de l'outil de travail 16

4. Copie de données informatiques.....16

5. Confidentialité et protection des données.....17

14. Application 17

15. Evolution..... 17

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

CHARTE D'UTILISATION DES MOYENS D'INFORMATIONS

1. Préambule et Organisation interne

La présente charte a pour objectif de formaliser les règles d'utilisation et de sécurité du système d'information de la **MFR Annecy.**

Les équipements informatiques, fournis par la **MFR Annecy,** sont dédiés à la réalisation des diverses missions et obligations légales de l'établissement.

Ces équipements sont de natures diverses : ordinateurs et smartphones.

De façon générale, le terme "ressources informatiques" correspond aux équipements, aux moyens de stockage, aux moyens informatiques ou de gestion locale ainsi qu'à ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par la **MFR Annecy.**

Les "services internet" correspondent à la mise à disposition par la **MFR Annecy** de moyens d'échanges et d'informations.

Les personnes utilisant ou ayant accès aux ressources informatiques, au réseau et aux services Internet sont appelées "utilisateurs".

Les administrateurs systèmes et/ou la direction des systèmes d'information (DSI) sont responsables techniquement de la sécurité et du bon fonctionnement des infrastructures informatiques et téléphoniques placées sous leur responsabilité.

Bien que les ordinateurs portables et/ou périphériques informatiques (smartphone, clé USB ...etc.) peuvent être emmenés à domicile, le matériel confié reste la propriété de la **MFR Annecy.** Sa restitution est obligatoire en cas de départ de l'utilisateur ou sur simple demande écrite de la DSI.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

2. Protection des Données Personnelles et droit applicable

1. Accès aux données à caractère personnel

Je soussigné/e Monsieur/Madame _____,

Exerçant les fonctions de _____

au sein de la **MFR Annecy** étant à ce titre amené/e à accéder à des données à caractère personnel,

déclare reconnaître la confidentialité des dites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des utilisateurs non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- Ne divulguer ces données qu'aux utilisateurs dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de utilisateurs privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- M'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- En cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

2. Traitement de données à caractère personnel

En tant qu'utilisateur, la **MFR Annecy** est amenée à collecter et traiter vos données à caractère personnel :

- Nom
- Prénom
- Coordonnées
- Date et lieu de naissance
- Carte d'identité
- Localisation : Collectivité
- Fonction : poste occupé
- Vie familiale
- Expériences et certifications professionnelles
- Fiches de paie
- RIB
- RQTH
- Dossiers médicaux
- Extrait N° 3 du casier judiciaire
- Numéro de sécurité sociale
- Permis de conduire

L'objectif principal de la collecte de vos données à caractère personnel sert à votre recrutement et à la constitution de votre dossier RH.

La **MFR Annecy** s'engage à ce que vos données soient traitées dans le respect des finalités précitées ainsi que pour des finalités qui leur sont compatibles.

Dans le respect du principe de minimisation des données traitées, instauré par le RGPD, la **MFR Annecy** s'engage à ce que les données collectées soient adéquates, pertinentes et non excessives par rapport à ces finalités.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

3. Bonnes pratiques

1. Bien choisir ses mots de passe

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne. Choisissez des mots de passe composés de minimum *12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux)* n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire.

2. Mettre à jour régulièrement vos logiciels

Dans chaque système d'exploitation* (Android, IOS, MacOs, Linux, Windows...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs* des mises à jour* de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

3. Bien connaitre ses utilisateurs et ses prestataires

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » * et les droits dits « d'administrateur » *.

- Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu...), prenez un compte utilisateur. Il répondra parfaitement à vos besoins.
- Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels...).

4. Effectuer des sauvegardes régulières

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer par suite d'un dysfonctionnement de votre système d'exploitation ou à une attaque.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

5. Sécuriser l'accès Wi-Fi

L'utilisation du Wi-Fi est une pratique courante. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des utilisateurs d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes malintentionnées. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

6. Être aussi prudent avec son smartphone qu'avec son ordinateur

Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique :

- N'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;

- En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;

- Effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;

- Ne préenregistrez pas vos mots de passe.

7. Protéger ses données lors de ses déplacements

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation. Il convient de se référer au passeport de conseils aux voyageurs édité par l'ANSSI.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

8. Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées...). Lorsque vous recevez des courriels, prenez les précautions suivantes :

- L'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail ;

- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts ;

- Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence ;

- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing » * ;

- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;

- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

9. Télécharger ses programmes sur les sites officiels des éditeurs

Vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie*. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

10. Être vigilant lors d'un paiement sur internet

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- Assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;
- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple

11. Séparer les usages personnels des usages professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels. Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette, etc.) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle pose des problèmes en matière de sécurité des données (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur). Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- Ne faites pas suivre vos messages électroniques professionnels sur des services et/ou adresses de messagerie utilisés à des fins personnelles ;
- N'hébergez pas de données professionnelles sur des équipements personnels (terminaux, périphériques, unités de stockage, téléphone, etc.) non validés par le responsable informatique ;
- N'hébergez pas de données professionnelles sur des moyens personnels de stockage en ligne ;
- De la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise. Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Les données que vous laissez sur Internet vous échappent instantanément. Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel. Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- Soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires ; pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;

- Ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;

- Pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité (Cf. Guide de la CNIL sur la sécurité des données personnelles) ;

- Enfin, utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...). Source : https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

4. Accès aux ressources informatiques

Les ressources informatiques et téléphoniques, le réseau et les services Internet sont destinés à l'activité professionnelle des utilisateurs du site conformément à la législation en vigueur.

L'utilisation des ressources informatiques communes et la connexion d'un équipement sur le réseau sont soumises à l'autorisation des administrateurs. Ces autorisations sont strictement personnelles et, en aucun cas ne peuvent être cédées, même temporairement, à un tiers.

En cas de non-respect de la présente charte, elles peuvent être annulées à tout moment. Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée. Seuls les terminaux préconisés par la DSI sont aptes à être connectées et à avoir accès aux services.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

5. Règles d'utilisation et de sécurité

Tout utilisateur est responsable de l'usage qu'il fait des ressources informatiques et du réseau auxquels il a accès. Il a le devoir de s'informer des règles de sécurité générales et propres au site auprès des administrateurs systèmes et réseaux. A son niveau, il a aussi, la charge de contribuer à la sécurité générale en respectant les règles d'utilisation, de sécurité et de bon usage. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement.

Il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs ; il lui appartient de sauvegarder ses données en utilisant les différents moyens de copie à sa disposition.

- Il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,
- Il doit respecter les règles en vigueur au sein de la **MFR Annecy** pour toute installation de logiciel,
- Il choisit des mots de passe sûrs et gardés secrets qu'en aucun cas il ne doit communiquer à des tiers (se référer au Guide des 12 Bonnes pratiques de l'ANSSI).
- Il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, quel que soit le type de matériel employé,
- Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,
- Il ne doit pas tenter de lire, modifier, copier ou détruire des données dont il n'a pas la responsabilité, sauf autorisation explicite,
- Il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter ou le verrouiller,
- Il ne doit pas gaspiller volontairement des ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseau, occupation de serveurs distants, etc.).
- Nul ne peut modifier un équipement commun, tant du point de vue matériel que logiciel, ni connecter un équipement au réseau sans l'accord explicite de l'administrateur,
- La connexion d'un équipement sur le réseau est soumise à l'accord de l'administrateur réseaux. La présente charte s'applique alors à cet équipement.
- Il doit, lors de son départ définitif de la **MFR Annecy,** détruire ses données privées. S'il ne s'y astreint pas, leur suppression sera réalisée de droit sans préavis.
- Par ailleurs, l'utilisateur ne doit ni installer ni utiliser de logiciels à caractère ludique.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

6. Règles de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques et téléphoniques doit être limité à ceux qui leur sont propres et à ceux qui sont publics ou partagés.

En particulier, il est illicite, sauf accord exprès du propriétaire, de prendre connaissance d'informations détenues par d'autres utilisateurs même si ceux-ci ne les ont pas protégées. Cette règle s'applique également aux échanges privés de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés ou du règlement général sur la protection des données, il devra auparavant en avoir fait la demande au Relai à la Protection des Données et/ou à notre Délégué à la Protection des Données : adresse en attente Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

En utilisant le service de courrier électronique mis à sa disposition par la **MFR Annecy** l'utilisateur est informé de l'existence de dispositifs automatisés de détections de pourriels (ou spams) et de courriels vecteurs de codes malveillants. Il en accepte le principe, sans aucune garantie de résultat.

7. Respect de la législation concernant la propriété intellectuelle

La reproduction, la représentation ou la diffusion d'une œuvre de l'esprit ou d'une création protégée au titre de droits voisins est soumise au respect des droits de propriété intellectuelle et nécessite une cession et/ou une autorisation émanant des titulaires des droits patrimoniaux et moraux prévus par le Code de la Propriété Intellectuelle, sous peine de constituer le délit de contrefaçon de droit d'auteur.

De même, les signes distinctifs et inventions étant susceptibles de protection au titre d'un droit de propriété intellectuelle, leur reproduction, représentation ou diffusion est susceptible de constituer, à défaut de telles cessions et/ou autorisations, le délit de contrefaçon de marque ou de brevet.

En ce qui concerne plus particulièrement la reproduction et/ou l'utilisation d'un logiciel, il est rappelé qu'en l'absence d'autorisation du titulaire des droits de propriété intellectuelle sur ce logiciel ou en cas de non-respect des conditions et limites définies par celui-ci (en ce qui concerne notamment les copies de sauvegarde), cette reproduction et/ou utilisation peut également être constitutive du délit de contrefaçon.

Il est enfin rappelé que les bases de données et les contenus en ligne sont protégés au bénéfice de leur auteur, outre par le droit d'auteur, par un droit spécifique.

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

8. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques, sniffer...

La sauvegarde des données stockées sur l'ordinateur reste de la responsabilité de l'utilisateur final. Toute perte due à une mauvaise utilisation ou à une défaillance de la machine n'est pas de la responsabilité de la **MFR Annecy.**

En cas de casse, détérioration ou vol du matériel :

- En dehors de l'établissement (hors délégation de mission), la responsabilité civile de l'emprunteur sera utilisée pour réparer ou remplacer le matériel,
- Sur le lieu de travail ou en délégation de mission, ce sera l'assurance de la **MFR Annecy** qui entrera en jeu.

La réparation d'une panne résultant d'une usure « normale » de la machine sera prise en charge par la **MFR Annecy.**

9. Usage des services internet

Tout utilisateur qui ne se sera pas conformé aux règles de bons usages engagera sa responsabilité en cas de détériorations d'informations ou d'infractions aux dispositions en vigueur.

La création ou l'usage de tout service d'échange d'informations, matériel ou logiciel, local ou hébergé, est soumis à l'accord de l'administrateur, se prononçant après avis du délégué à la protection des données (dans le cas de service en ligne) et de la Direction.

10. Droits et devoirs spécifiques des administrateurs systèmes et/ou réseaux

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés par les administrateurs systèmes et/ou réseaux dans le respect de la législation applicable, notamment de la loi sur l'informatique & les libertés ainsi que du règlement général sur la protection des données, et de la jurisprudence.

- Tout administrateur systèmes et/ou réseaux a le droit :

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

- D'accéder, sur les systèmes ou les réseaux qu'il administre, aux informations nécessaires à des fins de diagnostic et d'administration du système ou du réseau, en respectant scrupuleusement la confidentialité de ces informations et en s'efforçant de ne pas les altérer,
- D'établir des procédures de surveillance de toutes les tâches exécutées sur les machines, afin de déceler les violations ou les tentatives de violation de la présente charte,
- De prendre, en cas d'infraction à la charte, des mesures conservatoires, si l'urgence l'impose, sans préjuger des sanctions qui pourraient en résulter.
    - Il est informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible.

    - Tout administrateur systèmes et/ou réseaux à le devoir :

        - D'informer les utilisateurs, de les sensibiliser aux problèmes de sécurité informatique et de leur faire connaître les règles de sécurité à respecter,
        - De respecter les règles de confidentialité, en limitant l'accès aux informations strictement nécessaires et en respectant le "secret professionnel".
        - De faire respecter la présente charte.

11. HADOPI

Il est strictement interdit de téléchargez illégalement (*pirater*) des films ou de la musique à l'aide du système informatique de la **MFR Annecy,** vous pouvez recevoir un avertissement de la Hadopi. Ce 1er avertissement vous sera envoyé par mail. Après 2 avertissements, vous risquez des poursuites pénales et une amende.

12. Infraction à ces règles

Tout utilisateur n'ayant pas respecté ces règles est passible d'interdiction d'accès au réseau, de fermeture immédiate de son compte, de sanctions internes à la **MFR Annecy** et/ou de poursuites judiciaires selon le cas.

Pour information le code pénal rappel les sanctions en cas de non-respect des Données Personnelles :
Article 226-17 du Code pénal

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011

"Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 (...) est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende".

13. Télétravail

Le présent paragraphe définit les modalités de sécurisation du télétravail au sein de la **MFR Annecy.** Conformément aux articles L 1222-9 à 1222-11 du code du travail et L5213.10 du code du travail.

1. Accès à internet

L'utilisateur en situation de télétravail doit disposer, à son domicile, d'une connexion internet sécurisée afin d'accéder au SI de la **MFR Annecy** et garantir la sécurité des données à caractère personnel traitées. La connexion internet de chaque utilisateur en situation de télétravail doit être propre à l'usage professionnel et doit être protégée par un hotspot qui isole l'accès des autres membres de la famille et des visiteurs.

L'utilisateur en situation de télétravail devra changer le nom et le mot de passe de sa connexion internet en veillant à respecter les instructions du paragraphe 3.1 relatif aux bonnes pratiques en matière de choix de mots de passe.

2. Mot de passe

L'accès à la connexion internet et au SI doit être protégé par mot de passe individuel. Ces mots de passe doivent être gardés confidentiel par l'utilisateur afin de permettre le contrôle et la sécurité de l'activité de chacun.

Les mots de passe doivent être mémorisé et ne doivent pas être écrit sous quelque forme que ce soit. Ils ne doivent pas être transmis ou confiés à un tiers ou être rendu accessible.

Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

3. Sécurisation de l'outil de travail

L'utilisateur en situation de télétravail ne doit pas installer, copier, modifier des logiciels sur son poste informatique sans l'accord du service informatique (ou du responsable hiérarchique) en raison notamment du risque de virus informatiques.

Chaque outil informatique devra être sécurisé par un antivirus et un VPN afin de limiter les risques d'attaque informatique.

4. Copie de données informatiques

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

L'utilisateur en situation de télétravail doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données.

(ex : vol de clé USB, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles, ...).

5. Confidentialité et protection des données

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation. Il s'engage à prendre toutes les précautions utiles pour éviter qu'elles ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité.

L'utilisateur en situation de télétravail doit respecter les règles de confidentialité, de protection des données et de sécurité.

Depuis son domicile, l'utilisateur en situation de télétravail doit également et impérativement respecter les règles de la Charte informatique en vigueur.

14. Application

La présente charte s'applique à l'ensemble du personnel de la **MFR Annecy** tous statuts confondus, et plus généralement à l'ensemble des utilisateurs, permanents, temporaires ou visiteurs, utilisant les moyens informatiques situés sur les sites de la **MFR Annecy.**

L'accès aux ressources informatiques de la **MFR Annecy,** notamment l'usage des identifiants remis à l'utilisateur, implique l'acceptation pleine et entière de la présente charte.

Les informations recueillies par la **MFR Annecy** font l'objet d'un traitement informatique destiné à assurer la gestion des autorisations d'accès au système d'information de la **MFR Annecy** et à Internet.

Conformément à la loi « Informatique et Libertés » et au « Règlement Général sur la Protection des Données », vous bénéficiez des droits d'accès, de rectification, de suppression « droit à l'oubli » et de portabilité aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, merci d'adresser votre demande écrite à :

Lucile Capelle (adresse mail à venir).

15. Evolution

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace

La présente charte est rédigée dans l'intérêt de chacun des utilisateurs et manifeste la volonté de la **MFR Annecy** d'assurer un développement et une utilisation harmonieuse et homogène de son système d'information.

Chaque utilisateur, destinataire de la présente charte, est donc invité à transmettre à la direction toute proposition de modification ou d'ajout, dont il a pu constater l'intérêt dans le cadre de sa pratique professionnelle.

La présente charte sera régulièrement mise à jour par la direction et pourra faire l'objet d'adaptations spécifiques en fonction des catégories d'utilisateurs concernés.

Je soussigné_____, adhère à la charte d'utilisation des moyens d'informations ci-dessus en date du _____ / _____ / _____.

Pour la MFR Annecy

PASTORELLI Laurence, directrice

L'utilisateur :

NOM / PRENOM / FONCTION

Publication soumise aux droits d'auteur | Propriété exclusive de myDigitplace | Toute reproduction interdite sauf autorisation expresse de myDigitplace
Raison sociale : GA MA NEGOCE (MYDIGITPLACE) - Responsable : GARIN Jean Baptiste 06 64 08 98 50 contact@mydigitplace.com
Siège social : 3 bis, impasse des flamboyants 31600 LHERM - RCS : Toulouse 82197084500011