CHARTE INFORMATIQUE NODYA GROUP

INTRODUCTION

NODYA GROUP met en œuvre un système d'information et de communication nécessaire à l'exercice de l'activité de conseil et d'édition de logiciel des sociétés affiliées AYDON et DIGGLERZ. Elle met ainsi à disposition des collaborateurs du groupe des outils informatiques, et de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de *NODYA GROUP* et de ses filiales. Elle a notamment pour objet de préciser les droits et devoirs des Utilisateurs.

Elle a également pour objet de sensibiliser les Utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite aux Utilisateurs. L'imprudence, la négligence ou la malveillance d'un Utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de *[« l'Institution », « l'Organisme », « la Société »…]*.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

Le Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018. Le RGPD, complété par la nouvelle Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée du 14 juin 2018, impose les conditions dans lesquelles des traitements de données à caractère personnel peuvent être réalisés. Cette réglementation ouvre aux personnes concernées par les traitements un droit d'information, d'accès, de rectification, d'effacement, de portabilité et d'opposition des données enregistrées sur leur compte.

NODYA GROUP a désigné un Délégué à la Protection des Données à caractère personnel (DPO). Ce dernier a pour mission de veiller au respect des dispositions du RGPD Il a pour rôle de s'assurer de la conformité juridique des traitements.

Il est obligatoirement consulté par le responsable de traitement préalablement à la création d'un fichier. Le ***« Responsable de Traitement »*** est celui qui détermine les finalités et les moyens du traitement, c'est celui qui a pris l'initiative du traitement. A ce titre, *NODYA GROUP* est Responsable de Traitement.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de *NODYA GROUP* au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet de *NODYA GROUP*.

Le correspondant veille au respect des droits des personnes citées ci-dessus En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPO (Laurent GERAY l.geray@nodya-group.com directeur général de *NODYA GROUP*).

CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout Utilisateur du système d'information et de communication de *NODYA GROUP* pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des Utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet (http://www.nodya-group.com\charteinformatique) de *NODYA GROUP*. Elle est systématiquement remise à tout nouvel arrivant.

Des actions de communication internes sont organisées régulièrement afin d'informer les Utilisateurs des pratiques recommandées.

Quelques définitions :

On désignera sous le terme *« **Utilisateur »*** toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de *NODYA GROUP* et à les utiliser : employés, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....

Les termes *« **Outils Informatiques et de Communication** »* recouvrent tous les équipements informatiques, de télécommunications et de reprographie de *NODYA GROUP.*

REGLES D'UTILISATION DU SYSTEME D'INFORMATION DE *NODYA GROUP*

Chaque Utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par *NODYA GROUP.*

1. Les modalités d'intervention du service de l'informatique interne

Le service de l'informatique interne assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de *NODYA GROUP.* Le personnel de ce service dispose d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques et respectent les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à traiter dans le cadre de leurs fonctions.

2. L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte *("login"* ou identifiant) fourni à l'Utilisateur lors de son arrivée au sein de NODYA *GROUP.* Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels.

Actuellement, le mot de passe doit être composé de 8 caractères minimum combinant majuscules, minuscules, chiffres et caractères spéciaux. Il ne doit comporter ni le nom, prénom, date de naissance ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement (6 mois). A défaut, l'Utilisateur risque d'assister à un blocage de son compte.

L'authentification prévoit une restriction de l'accès au compte mise en place par le service de l'informatique interne (Verrouillage du compte après 5 échecs).

3. Les règles de sécurité

Tout Utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique interne de *NODYA GROUP* toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe à un tiers.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas enregistrer ses mots de passe dans son navigateur sans mot de passe maître.
- Ne pas stocker ses mots de passe dans un fichier clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
- Ne pas utiliser le même mot de passe pour des accès différents.
- Ne pas s'envoyer par courriel ses propres mots de passe.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de *NODYA GROUP.*
- Verrouiller son ordinateur dès qu'il quitte son poste de travail même pour un temps limité.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Effectuer des sauvegardes régulières et enregistrer les copies sur disque dur externe, CD, DVD.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par *NODYA GROUP.*
- Ne pas mener d'actions engageant la responsabilité juridique ou financière de la Société en répondant par exemple à un courriel.

Règles de sécurité propres au smartphone :

- N’installer que des applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Il faut éviter d’installer les applications qui demandent l’accès à des données qui ne sont pas nécessaires à leur fonctionnement.
- En plus du code PIN qui protège sa carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l’accès à son terminal et le configurer pour qu’il se verrouille automatiquement.

En tout état de cause, l’Utilisateur doit séparer les usages personnels des usages professionnels :

- Ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles.
- Ne pas héberger de données professionnelles sur ses équipements personnels (clés USB, téléphone…) ou sur des moyens personnels de stockage en ligne.
- Eviter de connecter des supports amovibles personnels (clés USB, disques durs externes…) aux ordinateurs de la Société.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au système d'information de *NODYA GROUP* sans l'accord préalable du service informatique interne.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre *NODYA GROUP* et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

MOYENS INFORMATIQUES ET MESURES DE CONTROLE

1. Configuration du poste de travail

Dans le cas ou NODYA GROUP met à disposition un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L'Utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un *« Equipement Nomade »).*
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord du service informatique interne.

2. Equipements Nomades et procédures spécifiques aux matériels de prêt

- **Equipements Nomades**

On entend par *« **Equipements Nomades** »* tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc…).

Sauf réserve technique particulière, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur doit être physiquement attaché à l'aide de l'antivol prévu à cet effet (sauf quand l'Utilisateur est physiquement présent dans son bureau).

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

- **Procédures spécifiques aux matériels de prêt**

L'Utilisateur doit renseigner et signer un registre, tenu par le service informatique interne, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (ex : vidéoprojecteur, hautparleur audio). Il en assure la garde et la responsabilité et doit informer le responsable informatique en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

3. Internet

Les Utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

4. Messagerie électronique

- **Conditions d'utilisation**

La messagerie mise à disposition des Utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'Utilisateur ni la sécurité du réseau informatique de *NODYA GROUP.*

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

NODYA GROUP s'interdit d'accéder aux dossiers et aux messages identifiés comme

« Personnel » dans l'objet de la messagerie de l'Utilisateur.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique interne, et validées par la direction générale :

- Volumétrie de la messagerie,

- Taille maximale de l'envoi et de la réception d'un message,

- Nombre limité de destinataires simultanés lors de l'envoi d'un message,

- Gestion de l'archivage de la messagerie.

Les Utilisateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'Utilisateur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

- **Consultation de la messagerie**

En cas d'absence d'un collaborateur et afin de ne pas interrompre le fonctionnement du service, le service informatique interne de *NODYA GROUP* peut, ponctuellement, transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages du collaborateur. Le collaborateur concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un Utilisateur (longue maladie), le chef de service peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

- **Courriel non sollicité**

NODYA GROUP dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

- **Contenu du courriel : pièces jointes, liens**

Il est strictement interdit à l'Utilisateur d'ouvrir des pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que leur envoient habituellement leurs contacts.

De même, si des liens figurent dans un courriel, il est fortement recommandé aux Utilisateurs de passer leur 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). L'Utilisateur pourra ainsi en vérifier la cohérence.

En tout état de cause, l'Utilisateur doit respecter les règles suivantes :

- Ne jamais répondre par courriel à un demande d'informations personnelles ou confidentielles (par exemple : code confidentiel et numéro de carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Impôts pour récupérer les données des personnes concernées. Il s'agit d'attaques par hameçonnage ou « pishing ».

- Ne pas ouvrir et ne pas relayer de messages de type chaînes de lettre, appels à la solidarité, alertes vitales…

5. Téléphone

Dans certains cas*, NODYA GROUP* met à disposition des Utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation par les Utilisateurs des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

NODYA GROUP s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

NODYA GROUP s'interdit d'accéder à l'intégralité des numéros appelés via le système de téléphonie mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service informatique, sur demande du Président ou du Directeur général, se réserve le droit d'accéder aux numéros complets des relevés individuels.

6. Déplacements professionnels

L'emploi des Equipements Nomades facilite les déplacements professionnels mais fait peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de la Société.

C'est pourquoi, les Utilisateurs sont tenus de respecter les règles suivantes :

AVANT DE PARTIR EN MISSION

- N'utiliser que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission et ne contenant que les données nécessaires.
- Sauvegarder ces données, pour les retrouver en cas de perte.
- Emporter un filtre de protection pour son ordinateur si l'Utilisateur compte profiter des trajets pour travailler.
- Apposer un signe distinctif (par exemple, une pastille de couleur) sur ses appareils pour s'assurer qu'il n'y a pas eu d'échange pendant le transport,
- Vérifier que ses mots de passe ne sont pas préenregistrés.

PENDANT LA MISSION

- Garder ses appareils, supports et fichiers avec soi, pendant son voyage comme pendant le séjour (ne pas les laisser dans un bureau ou un coffre d'hôtel).
- Désactiver les fonctions Wi-Fi et Bluetooth de ses appareils.
- Retirer la carte SIM et la batterie s'il est contraint de se séparer de son téléphone.
- Informer son entreprise en cas d'inspection ou de saisie de son matériel par des autorités étrangères.
- Ne pas utiliser les équipements offerts à l'Utilisateur s'il ne peut pas les faire vérifier par un service de sécurité de confiance.
- Eviter de connecter ses équipements à ses postes qui ne sont pas de confiance (par exemple : si l'Utilisateur a besoin d'échanger des documents lors d'une présentation commerciale, utiliser une clé USB destinée uniquement à cet usage et effacer ensuite les données avec un logiciel d'effacement sécurisé).
- Refuser la connexion d'équipements appartenant à des tiers à ses propres équipements (smartphone, clé USB, baladeur…)

APRES LA MISSION

- Effacer l'historique des appels de navigation.
- Changer les mots de passe que l'Utilisateur a utilisés pendant le voyage.
- Faire analyser ses équipements après la mission s'il le peut.
- Ne jamais utiliser les clés USB qui peuvent avoir été offertes lors de ses déplacements (salons, réunions, voyages…) : elles sont susceptibles de contenir des programmes malveillants.

7. Téléchargements

Si l'Utilisateur télécharge du contenu numérique sur des sites internet dont la confiance n'est pas assurée, il prend le risque d'enregistrer sur son ordinateur des programmes qui contiennent des virus. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de sa machine pour notamment espionner les actions réalisées sur son ordinateur, voler ses données personnelles, lancer des attaques.

Afin de veiller la sécurité de sa machine et de ses données, l'Utilisateur doit respecter les règles suivantes :

- Télécharger ses programmes sur les sites des éditeurs ou d'autres sites de confiance.
- Penser à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires.
- Rester vigilant concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens.
- Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

8. Paiements sur internet

Avant d'effectuer un paiement en ligne, il est nécessaire que l'Utilisateur procède aux vérifications sur le site Internet :

- Contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de son navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- S'assurer que la mention « https:// » apparaît au début de l'adresse du site Internet.
- Vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

9. L'utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel au comité social économique utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle. Ils disposent d'une adresse électronique dédiée (representants@nodya-group.fr).

ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information de la Commission, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour *NODYA GROUP* et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée…).

2. Les systèmes automatiques de traçabilité

Le service informatique de la *NODYA GROUP* opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement.

Le service informatique est le seul Utilisateur de ces informations qui sont effacées à l'expiration d'un délai de trois mois.

3. Gestion du poste de travail

A des fins de maintenance informatique, le service informatique interne de *NODYA GROUP* peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'Utilisateur qui aura préalablement été informé de la finalité de l'opération.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun Utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'Utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.

Les comptes et les données personnelles de l'Utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'Utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

- Dans un premier temps, en un rappel à l'ordre émanant du service informatique interne, après avis du président ou directeur général, en cas de non-respect des règles énoncées par la charte ;

- Dans un second temps, et en cas de renouvellement, après avis du président ou du directeur général et du supérieur hiérarchique du collaborateur, en des sanctions disciplinaires adoptées après saisine du comité consultatif paritaire restreint.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

ENTREE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée après information et consultation du comité consultatif paritaire.

Elle est applicable à compter du 01/05/2018.

ANNEXES

DISPOSITIONS LEGALES APPLICABLES

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiées par la loi n°2004-801 du 6 août 2004, dans sa version consolidée du 14 juin 2018 (nouvelle LIL).

Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, entré en vigueur le 25 mai 2018 (RGPD).

Dispositions Pénales :
- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels. Disposition pénale : art L.335-2 du Code pénal.