REGLEMENT INTERIEUR ACADEMIE FIVES NORDON

TITRE 1 – DISPOSITIONS GENERALES

ARTICLE 1 : OBJET DU REGLEMENT

La Direction de l'Académie Fives Nordon fixe ci-après :

- Les règles générales et permanentes relatives à la discipline sur l'ensemble des sites rattachés au SIREN de Fives Nordon (numéro 433948031) ainsi que tous lieux extérieurs sur lesquels se déroulent les formations de l'Académie Fives Nordon.

- Les mesures d'application de la réglementation en matière d'hygiène et de sécurité pendant les actions de formation dispensées par l'Académie Fives Nordon.

ARTICLE 2 : CHAMP D'APPLICATION

Parce qu'il est destiné à organiser la vie durant la formation professionnelle, ce règlement s'applique à l'ensemble des stagiaires inscrits dans un dispositif de formation quelles qu'en soit la nature et la durée.

Le contenu de ce règlement intérieur s'applique sur l'ensemble des sites rattachés au SIREN de Fives Nordon (numéro 433948031) ainsi que tous lieux extérieurs sur lesquels se déroulent les formations de l'Académie Fives Nordon.

TITRE 2 – DISPOSITIONS RELATIVES A L'HYGIENE, LA SANTE ET A LA SECURITE

Lorsque les formations dispensées par l'Académie Fives Nordon se déroulent sur les sites de Fives Nordon, les dispositions du règlement intérieur de Fives Nordon relatives à l'hygiène, la santé et la sécurité sont pleinement applicables aux stagiaires de l'Académie Fives Nordon.

Ces dispositions sont les suivantes (art 3 à 16) :

ARTICLE 3 : OBLIGATIONS GENERALES DE VIGILANCE ET DE SECURITE PESANT SUR LES STAGIAIRES

Il incombe à chaque stagiaire conformément aux instructions qui lui sont données par le formateur ou le coordinateur de l'Académie Fives Nordon, application du présent règlement intérieur et, le cas échéant, des notes de service qui le complètent, de prendre soin, en fonction de sa formation, de ses possibilités, de sa sécurité et de sa santé ainsi que celle des autres personnes concernées du fait de ses actes ou des omissions au travail.

Des notes de service fixent les consignes chaque fois qu'il y a lieu ; elles complètent, en tant que de besoin, les prescriptions définies ci-après, applicables dans tous les cas. Les stagiaires ont l'obligation de respecter toutes les consignes de sécurité spécifiques à cette exécution.

ARTICLE 4 : RESPECT DES MESURES D'HYGIENE, DE SANTE ET DE SECURITE

La prévention des risques professionnels est impérative, c'est pourquoi l'ensemble des règles, mesures et consignes applicables en matière d'hygiène, de santé et de sécurité doivent être parfaitement connues des stagiaires de l'Académie Fives Nordon et strictement respectées.

En outre, les stagiaires ont l'obligation de respecter toutes les consignes particulières qui leur sont données par le personnel d'encadrement du stage pour l'exécution de leurs apprentissages et notamment les consignes de sécurité spécifiques à cette exécution.

Il appartient au personnel d'encadrement du stage de veiller au respect des mesures d'hygiène, de santé et de sécurité.

ARTICLE 6 : LAVABOS – TOILETTES

Les lavabos et cabinets d'aisance doivent être tenus en constant état de propreté par leurs utilisateurs, la Société Fives Nordon assurant le nettoyage régulier.

ARTICLE 7 : BOISSONS ALCOOLISESS – DROGUE – CIGARETTES

Il est strictement interdit aux stagiaires :

Il est strictement interdit au personnel :

- D'introduire et/ou de consommer sur les lieux de travail des produits alcoolisés et/ou des stupéfiants ;
- D'entrer ou de séjourner sur les lieux de travail sous l'emprise de stupéfiants ;
- D'entrer ou de séjourner sur les lieux de travail en état d'ébriété ;
- De fumer ou de vapoter dans tout lieu collectif, fermé et couvert.

Sur le site de NANCY les zones fumeurs sont restreintes à quelques emplacements spécifiques équipés de cendriers.

En dehors de ces zones il sera interdit de fumer et de vapoter sur le site de Nancy y compris dans les lieux non couverts et non fermés (*zone de convivialité, allées de circulation, points de rassemblements...).*

En raison de l'obligation faite au Chef d'Entreprise de prévenir ou de faire cesser immédiatement une situation dangereuse dans les locaux de l'Entreprise ou sur tout site sous notre responsabilité , dès lors que le comportement d'un stagiaire laisse présumer d'un état d'imprégnation alcoolique ou de consommation de stupéfiants (Exemples non exhaustifs : *troubles de l'élocution, de l'équilibre, du comportement, non-respect des règles de sécurité, odeur spécifique*..), le stagiaire concerné pourra être soumis à l'épreuve de l'alcootest et/ou du test de détection salivaire immédiate de drogues.

Le stagiaire qui en raison de son poste de travail peut être soumis à des risques spécifiques :

- Personnel travaillant sur l'un des postes listés sur la liste des postes à risques particuliers E6 LPRP y compris dans ses versions futures
- Personnel qui conduit des véhicules automobiles dans le cadre de l'exercice de son activité professionnelle

- Personnel qui intervient sur sites dits sensibles (INB, sites chimiques, pétroliers, gaz, tous chantiers industriels...)

Peut être soumis immédiatement à l'épreuve de l'alcootest et/ou du test salivaire de détection de stupéfiants de manière aléatoire, ainsi que tout collaborateur et stagiaire de l'entreprise et de l'Académie Fives Nordon.

Un (des) représentant(s) de l'Académie Fives Nordon présent(s) sur le lieu d'intervention est (sont) autorisé(s) à procéder à l'alcootest et au test salivaire en présence d'un témoin.

Le témoin sera en priorité un représentant du personnel, dès que cela sera possible.

Les personnes procédant à l'alcootest ou au test de détection salivaire immédiate sont tenues à la discrétion sur le résultat, hormis à l'égard de la Direction de Fives Nordon, du service RH et du service médical et des prescripteurs du stage.

Le stagiaire présentant un taux d'alcool supérieur à zéro ou un test salivaire attestant de la consommation préalable de stupéfiants, ou refusant de se soumettre à ce contrôle fera l'objet d'un retrait immédiat du stage et sera susceptible de sanctions telles que prévues au présent règlement.

Le stagiaire concerné pourra demander une contre-analyse, laquelle sera alors réalisée dans l'heure qui suit, par un laboratoire d'analyse médicale.

ARTICLE 8 : ACCIDENTS

Tout accident, même bénin, survenu au cours de la formation ou au cours du trajet aller et retour du domicile au lieu de travail doit être signalé au coordinateur de l'Académie.

ARTICLE 9 : DISPOSITIF DE PROTECTION ET DE SECURITE

Le stagiaire est tenu de connaître parfaitement les consignes relatives à l'utilisation des dispositifs de protection et de sécurité.

Il doit respecter les consignes générales et particulières de sécurité en vigueur sur les lieux du travail, ainsi que les dispositions mises en place dans l'Entreprise pour l'application des prescriptions prévues par la réglementation en vigueur en matière d'hygiène et de sécurité.

Il doit se conformer aux indications générales et permanentes du formateur.

Il a pour obligation, de maintenir en place les dispositifs de toute natures installés pour assurer la protection collective des travailleurs.

Tout stagiaire doit utiliser correctement les appareils ou dispositifs de protection individuels ou collectifs qui sont mis à sa disposition par l'Académie Fives Nordon, lorsqu'il exécute des travaux pour lesquels le port de ces dispositifs est obligatoire.

Il est rappelé que la liste des protections individuelle : se compose (selon les lieux et travaux d'interventions) :

- D'un casque de sécurité
- De chaussures de sécurité
- De vêtements de travail

- De gants
- De protections auditives
- De harnais de sécurité
- De stop chute
- De masques anti-poussière
- De masques de soudeur
- De lunettes de soudage et de meulage
- De tabliers
- De vêtements de pluie
- De kits amiante

Et qu'un complément pourra être apporté en fonction de la particularité des travaux (exemple : travaux sur ou à proximité de l'eau, travaux amiante).

Toute défectuosité ou toute détérioration de ces dispositifs doit être signalée immédiatement au formateur.

Le formateur présente les règles de sécurité applicables durant la formation au démarrage de l'action, et notamment la liste des équipements de protection individuelle (EPI) devant être portés par les stagiaires pendant toute ou une partie de la formation.

Tout manquement au port des EPI ou aux règles de sécurité entrainera le renvoi du stagiaire de la formation sans possibilité de réintégration ni de remboursement de la formation.

ARTICLE 10 : PROCEDURE DE RETRAIT

Tout stagiaire ayant un motif raisonnable de penser qu'une situation présente un danger grave et imminent pour sa vie ou sa santé (exemple : défectuosité dans les moyens de protection) peut se retirer de son apprentissage.

Il avertira immédiatement le formateur et/ou le coordinateur de l'Académie Fives Nordon, de l'existence de ce danger et pourra, s'il le souhaite, établir une note relatant l'événement.

ARTICLE 12 : PERIL – DISPOSITIF DE LUTTE CONTRE L'INCENDIE

En cas de péril, notamment d'incendie, l'évacuation des stagiaires s'effectue, conformément aux consignes de sécurité affichées à cet effet.

Les stagiaires doivent notamment veiller au libre accès aux moyens et matériel de lutte, ainsi qu'aux issues de secours.

ARTICLE 13 : SUBSTANCES ET PREPARATIONS DANGEREUSES

Tout stagiaire affecté à un apprentissage l'exposant à des substances ou préparations dangereuses est tenu d'utiliser ou de manipuler ces substances ou préparations, conformément aux instructions qui lui sont données par le formateur et définies dans le cadre des consignes établies.

Les stagiaires sont informés, par leur formateur, des risques auxquels leur travail peut les exposer et les dispositions prévues pour les éviter, avant le début d'activité.

ARTICLE 15 : ARMES

L'introduction d'armes dans l'enceinte des lieux de formation de l'Académie Fives Nordon est interdite.

ARTICLE 16 : HYGIENE DANS LES LIEUX DE FORMATION

Les locaux et places de travail ainsi que leurs dépendances devront être maintenus en parfait état de propreté. Il en sera de même en ce qui concerne l'ensemble de l'Etablissement.

Le stagiaire devra notamment s'abstenir de laisser sur tout lieu de travail détritus, vieux papiers, mégots, bouchons d'oreilles usagers etc ...

Les stagiaires seront tenus de respecter strictement les consignes de nettoyage qui leur seront données relatives au lieu de formation. Chaque stagiaire devra tenir sa place en parfait état de propreté.

ARTICLE 17 : ATTITUDE, DISCIPLINE ET REGLES DE VIE GENERALES

Les stagiaires sont tenus de faire preuve d'investissement dans le cadre de leur formation.

Le temps de formation est un investissement dans l'apprentissage et la montée en compétences offerte aux stagiaires.

La formation est également une opportunité de changer, durant une période donnée, de cadre de travail, de faire des rencontres professionnelles, d'échanger entre pairs sur les cas et pratiques professionnelles.

La formation est un lieu riche dont les stagiaires doivent êtres les principaux moteurs.

A ce titre, il est demandé aux stagiaires de :

- Veiller à mettre leur téléphone en silencieux
- S'investir pleinement dans le temps de formation et éviter toute sollicitation externe (consultation d'outils NTIC notamment)
- Ne pas consacrer le temps de formation à une activité autre que celle dispensée par le formateur
- D'avoir une attitude d'écoute et de respect du formateur
- Respecter les autres stagiaires de la formation
- De prévenir en cas de retard ou d'absence.

Les stagiaires sont invités à se présenter en formation vêtus d'une tenue correcte (*vêtements couvrants, chaussures plates, pas de jupes pour toutes les formations nécessitant des mises en pratiques professionnelles).*

ARTICLE 18 : MAINTIEN ET UTILISATION DU MATERIEL

Chaque stagiaire a la responsabilité du maintien en bon état du matériel qui lui est confié dans le cadre de sa formation.

Les stagiaires sont tenus d'utiliser le matériel conformément à son objet : l'utilisation du matériel à d'autres fins, notamment personnelles, est interdite.

A l'issue de la formation, le matériel devra être nettoyé et rangé conformément aux règles de stockage communiquées par le formateur. Les espaces de travaux pratiques devront rester propres et ordonnés.

Toute défaillance du matériel devra immédiatement être communiquée au formateur.

Il est interdit de toucher aux machines, engins, moyens de transport ainsi qu'aux différents éléments des installations électriques sans être qualifié à cet égard.

Il est interdit aux stagiaires non qualifiés d'essayer de procéder à une réparation ou à un démontage sans autorisation.

Les outils et les équipements prévus pour la formation ne doivent être utilisés qu'en présence du formateur et sous sa surveillance.

Les outils et les équipements prévus pour la formation ne doivent pas être utilisés à des fins personnelles.

Toute utilisation d'un outillage autre que celui indiqué par le formateur ou du coordinateur de l'Académie Fives Nordon.

La constatation de vol, ou de toute perte, doit être portée sans délai à la connaissance du coordinateur de l'Académie Fives Nordon.

Dans le cas où seraient constatées des disparitions de produits, de matériels ou de documents au préjudice de l'organisme de formation, des stagiaires ou de toute personne présente dans l'organisme de formation ou de l'entreprise Fives Nordon, le coordinateur de l'Académie Fives Nordon se réserve le droit d'inviter les stagiaires à présenter le contenu des effets, objets, paquets ou sacs dont ils sont porteurs, après les avoir avertis de leur droit de s'opposer à une telle vérification ou d'exiger la présence d'un témoin.

L'accord des intéressés sera, dans la mesure du possible, recueilli en présence d'un salarié de l'organisme de formation.

En cas de refus, le coordinateur de l'Académie Fives Nordon se réserve le droit de faire appel à un Officier de Police Judiciaire.

En toute hypothèse, les modalités de ces fouilles préserveront la dignité et l'intimité des personnes.

ARTICLE 19 : ACCIDENT

Tout accident ou incident survenu à l'occasion ou en cours de formation doit être immédiatement déclaré par le stagiaire accidenté ou les personnes témoins de l'accident, au coordinateur de l'Académie Fives Nordon.

En fonction de la qualité et du statut du stagiaire, les déclarations règlementaires seront réalisées par l'organisme adéquat.

ARTICLE 21 : ACCES A L'ORGANISME

Sauf autorisation expresse du coordinateur de l'Académie Fives Nordon, les stagiaires ayant accès à l'organisme pour suivre leur stage ne peuvent :

- Y entrer ou y demeurer à d'autres fins.
- Y introduire, faire introduire ou faciliter l'introduction de personnes étrangères à l'organisme, ni de marchandises destinées à être vendues au personnel ou aux stagiaires.

TITRE 3 – DISPOSITIONS RELATIVES A L'ORGANISATION DE LA FORMATION

ARTICLE 22 : HORAIRES DE FORMATION/ ABSENCES

Les horaires collectifs de formation sont fixés par le coordinateur de l'Académie Fives Nordon et communiqués dans la convocation envoyée en amont de la formation. Les horaires s'imposent à chaque stagiaire et nulle initiative individuelle ne peut les modifier.

Le formateur ou le coordinateur de l'Académie Fives Nordon peut procéder à une modification des horaires. Il en informera les stagiaires et leurs entreprises ou organismes prescripteurs le cas échéant.

Les stagiaires sont tenus de respecter ces horaires de stage sous peine de l'application des dispositions suivantes :

- Lorsque les stagiaires sont des salariés en formation, l'organisme doit informer préalablement l'entreprise de ces absences, les heures de formation étant comptabilisées dans le temps de travail. Les absences doivent être justifiées sous peine d'une retenue sur salaire ;
- Lorsque les stagiaires sont demandeurs d'emploi rémunérés par l'État ou une région, les absences non justifiées entraîneront, en application de l'article R 6341-45 du Code du Travail, une retenue de rémunération proportionnelle à la durée des dites absences.

En cas d'évènements personnels prévisibles (*exemple : convocation d'une administration, rendez-vous médical spécialisé, etc...*), le stagiaire devra demander une autorisation d'absence **au responsable de l'organisme de formation, en respectant un délai de prévenance minimum de 48h**.

Cette autorisation ne vise pas les situations imprévisibles qui devront être portées à la connaissance du coordinateur de l'Académie Fives Nordon dans les plus brefs délais.

Les cas imprévisibles pour lesquels des autorisations de sortie peuvent être accordées sont les suivants :

- Stagiaire malade sur les lieux de formation et regagnant son domicile, après passage préalable à l'infirmerie si le site de formation en est doté ;
- Evénement familial grave survenant inopinément.

En cas de départ anticipé de la formation (***départ avant l'heure de fin initialement prévue),*** le stagiaire devra avoir signé avec le formateur ou le responsable de l'organisme de formation **un bon d'autorisation de sortie anticipée** (*modèle en annexe du présent règlement).* Ce bon sera conservé par le coordinateur de l'Académie Fives Nordon.

Tout départ ou absence non autorisé au préalable par du coordinateur de l'Académie Fives Nordon sera considéré comme une absence injustifiée.

Par ailleurs, les stagiaires sont tenus de remplir ou signer obligatoirement et régulièrement, au fur et à mesure du déroulement de l'action, l'attestation de présence, et, en fin de stage, le bilan de formation ainsi que l'attestation de suivi de stage.

TITRE 4 – DISPOSITIONS RELATIVES A L'ORGANISATION DE LA VIE COLLECTIVE

ARTICLE 23 : DEFINITION

Outre les règles relatives à l'organisation collective du travail définies ci-avant, il est nécessaire d'organiser la vie collective de formation afin d'assurer une coexistence ordonnée au sein de cet ensemble.

ARTICLE 24 : ENTREES ET SORTIES

Les entrées et sorties des stagiaires s'effectuent en empruntant les itinéraires et issues prévus à cet effet. Il est interdit de pénétrer dans les locaux ou d'en sortir, par toute autre issue.

Sauf dans les cas prévus par les dispositions légales ou conventionnelles ou autorisation du coordinateur de l'Académie Fives Nordon, l'entrée des locaux et des dépendances est interdite à toute personne étrangère à l'organisme ainsi qu'à tout salarié qui n'y est pas appelé par son travail ou ses fonctions.

ARTICLE 25 : UTILISATION DES OUTILS INFORMATIQUES ET TELEMATIQUES

Les règles d'utilisation des systèmes d'information sur les sites de Fives Nordon relèvent de la charte informatique de Fives Nordon, qui est annexée au présent règlement.

ARTICLE 26 : AFFICHAGES

Les affiches de service apposées dans les conditions légales et réglementaires sur les panneaux muraux d'expression réservés à cet effet ne devront pas être lacérées ou détruites.

Il est interdit de procéder sans autorisation à des affichages en dehors des emplacements prévus.

TITRE 5 – DISPOSITIONS RELATIVES AU TRAITEMENT DES DONNEES PERSONNELLES

L'organisme de formation est amené à solliciter des données personnelles en vue de la gestion des stagiaires, à savoir la gestion des dossiers d'indemnisation, la sollicitation d'aides diverses (garde d'enfants, mobilité, hébergement) pour les stagiaires, divers échanges avec les financeurs,

partenaires emploi, formateurs et équipe de l'Académie, l'accompagnement dans la recherche d'un stage avec des entreprises partenaires (liste non exhaustive).

Les données à caractère personnel enregistrées sont destinées uniquement à l'usage des services concernés et aux destinataires suivants : formateurs et équipes de l'Académie, associations et partenaires emplois, financeurs, entreprises partenaires (recherche stage ou accompagnement vers l'emploi, ex : transmission d'un CV).

Pour toute demande, le stagiaire pourra s'adresser au coordinateur de l'Académie Fives Nordon.

Le stagiaire peut demander auprès du responsable du traitement l'accès, la rectification ou l'effacement des données. En outre, le stagiaire peut introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL). »

TITRE 6 – DISPOSITIONS RELATIVES AUX MODALITES DE REPRESENTATION DES STAGIAIRES

ARTICLE 27 : REPRESENTATION DES STAGIAIRES

Lorsqu'une formation a une durée supérieure à 500 heures, l'élection d'un délégué titulaire et d'un délégué suppléant en scrutin uninominal à deux tours est organisée par le coordinateur de l'Académie Fives Nordon au plus tôt 20 heures, au plus tard 40 heures après le début du stage.

Tous les stagiaires sont électeurs et éligibles.

En cas d'impossibilité de désigner les représentants des stagiaires, le coordinateur de l'Académie Fives Nordon dresse un PV de carence qu'il transmet au préfet de région territorialement compétent.

Les délégués sont élus pour la durée de la formation. Leurs fonctions prennent fin lorsqu'ils cessent, pour quelque cause que ce soit, de participer à la formation.

Si le délégué titulaire et le délégué suppléant ont cessé leurs fonctions avant la fin de la session de formation, il est procédé à une nouvelle élection dans les conditions prévues aux articles R.6352-9 à R.6352-12 du code du travail.

Le rôle des représentants des stagiaires est de collecter et de communiquer toute remarque ou suggestion qui permet d'améliorer le déroulement de la formation (conditions d'accueil et de vie, ressources, matériel, ...).

Ils présentent toutes les réclamations individuelles ou collectives relatives à ces matières, aux conditions d'hygiène et de sécurité et à l'application du règlement intérieur.

TITRE 7 – DISPOSITIONS RELATIVES A LA DISCIPLINE

ARTICLE 28 : DEFINITION DES SANCTIONS ET PROCEDURES DISCIPLINAIRES

Tout manquement du stagiaire à l'une des prescriptions du présent règlement intérieur pourra faire l'objet d'une sanction.

Constitue une sanction au sens de l'article R. 6352-3 du Code du Travail toute mesure, autre que les observations verbales, prises par le coordinateur de l'Académie Fives Nordon, à la suite d'un

agissement du stagiaire considéré par lui comme fautif, que cette mesure soit de nature à affecter immédiatement ou non la présence de l'intéressé dans le stage ou à mettre en cause la continuité de la formation qu'il reçoit.

Les amendes ou autres sanctions pécuniaires sont interdites.

Selon la gravité du manquement constaté, la sanction pourra consister :

- Soit en un rappel à l'ordre ;
- Soit en un avertissement écrit ;
- Soit en une mesure d'exclusion définitive de la formation.

Aucune sanction ne peut être infligée au stagiaire sans que celui-ci ait été informé au préalable des griefs retenus contre lui.

Lorsque le coordinateur de l'Académie Fives Nordon envisage de prendre une sanction qui a une incidence, immédiate ou non, sur la présence d'un stagiaire dans une formation, il est procédé comme suit :

1° Le stagiaire est convoqué et informé de l'objet de la convocation. La convocation précise la date, l'heure et le lieu de l'entretien et la possibilité de se faire assister par le délégué de stage ou la personne de son choix.

Elle est écrite et est adressée par lettre recommandée ou remise à l'intéressé contre décharge.

2° Le responsable ou son représentant indique le motif de la sanction envisagée et recueille les explications du stagiaire.

La sanction fera l'objet d'une décision écrite et motivée, notifiée au stagiaire par lettre recommandée ou remise contre récépissé.

Le coordinateur de l'Académie Fives Nordon devra informer de la sanction prise :

- L'employeur, lorsque le stagiaire est un salarié bénéficiant d'un stage dans le cadre du plan de formation en entreprise.
- L'employeur et le financeur qui a pris à sa charge les dépenses de la formation, lorsque le stagiaire est un salarié bénéficiant d'un stage financé par un organisme paritaire ou lorsque le stagiaire est stagiaire de la formation professionnelle bénéficiant d'un stage financé par un partenaire emploi (France Travail) ou un partenaire régional.

La sanction n'interviendra pas moins d'un jour franc ni plus de quinze jours après l'entretien.

TITRE 8 – DISPOSITIONS RELATIVES AU HARCELEMENT MORAL, AU HARCELEMENT SEXUEL ET A LA VIOLENCE EN FORMATION ET AUX AGISSEMENTS SEXISTES

ARTICLE 29 : DISPOSITIONS RELATIVES AUX AGISSEMENTS SEXISTES, HARCELEMENT SEXUEL ET HARCELEMENT MORAL

L'Académie Fives Nordon prohibe tout agissement sexiste, actes de harcèlements moral ou sexuel :

- de la part de son personnel et du personnel présent sur les sites de formation envers ses stagiaires ;
- des stagiaires envers les formateurs, représentants de l'organisme de formation et toutes personnes présentes sur les sites de formations ;
- des stagiaires entre eux.

Tout stagiaire qui serait témoin ou victime de tels actes doit les faire remonter sans délai au coordinateur de l'Académie Fives Nordon qui prendra les mesures nécessaires.

Tout stagiaire ayant procédé à de tels actes est passible d'une sanction disciplinaire, dans le cadre de l'article 20 du présent règlement.

ARTICLE 30 : DISPOSITIONS RELATIVES AU PRINCIPE DE NEUTRALITE

Les lieux de formation de l'Académie Fives Nordon sont des lieux neutres.

Tout acte de prosélytisme, défini comme le zèle ardent pour recruter des adeptes et pour tenter d'imposer ses convictions, notamment religieuses ou politiques (non exhaustif), est interdit sur les lieux de formation de l'Académie.

Lorsque la formation pratique nécessite le port d'équipements de protection ou implique l'accès à des machines en mouvement comportant un risque d'entraînement, tout vêtement, ou accessoire gênant (ex non exhaustifs, bijoux, foulards, écharpe, pilosité importante...) empêchant le port des équipements de protection requis est interdit.

ARTICLE 31 : REVISIONS ET MODIFICATIONS

- Le règlement intérieur peut être modifié à tout moment en fonction des besoins de l'organisme de formation ou des évolutions législatives.
- Les stagiaires seront informés de toute modification et devront en prendre connaissance.

ARTICLE 32 : ACCEPTATION DU REGLEMENT

- En début de stage, les stagiaires devront lire et signer ce règlement intérieur pour en accuser réception et acceptation.

Fait à Nancy, le 20 janvier 2025

Signature du coordinateur de l'Académie Fives Nordon

CHARDIN Marjorie

Annexes :

- Bon d'autorisation de sortie anticipée
- Charte informatique de la société FIVES NORDON

AUTORISATION DE SORTIE ANTICIPEE

D'UN STAGIAIRE DE FORMATION

Je soussigné(e) ……, Coordinateur de l'Académie Fives Nordon autorise M/Mme …… (nom et prénom), stagiaire en formation …… (intitulé de la formation), du …./…./…. (JJ/MM/AAAA) au …./…./…. (JJ/MM/AAAA) à l'Académie Fives Nordon à quitter le stage à titre exceptionnel/régulièrement :

Le …. / …. / …. (JJ/MM/AAAA) de …. H …. à …. H …..

Le …. / …. / …. (JJ/MM/AAAA) de …. H …. à …. H …..

Au motif de : ……

Date et lieu

SIGNATURE et CACHET

fives

Charte d'utilisation du Système d'Information de Fives Nordon

Document interne

Sommaire

Glossaire 3
1. Objet de la Charte 4
2. Champ d'application de la Charte 4
3. Engagement de respect de la Charte et sanctions 4
4. Conditions générales d'utilisation des ressources 5
5. Règles de sécurité et de bon usage des ressources 7
   5.1. Postes de travail 7
   5.2. Internet 9
   5.3. Intranet, applications et serveurs internes 10
   5.4. Réseau Social d'Entreprise / de Groupe 10
   5.5. Messageries 10
   5.6. Terminaux mobiles 12
6. Traitement de données à caractère personnel 13
7. Contrôle des ressources 14
8. Entrée en vigueur de la Charte 15

Glossaire

Administrateur informatique : Toute personne responsable des actions d'administration ou d'exploitation des ressources du Système d'Information (installation, configuration, maintenance, support et évolution des ressources) ou des actions de sécurisation et de contrôle de ces ressources.

débrider un équipement (synonymes : jailbreaker / rooter un équipement) : Procédé consistant à éliminer les restrictions et sécurités pour déverrouiller des protections du système d'exploitation d'un équipement.

données : Ce terme désigne les fichiers, bases de données, images, sons, textes, vidéos, flux ainsi que les informations sous format oral et écrit, informatisé ou non.

données à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable (directement ou indirectement), nom, prénom, numéro de téléphone, numéro d'identification, données de localisation, identifiant en ligne, photographies …

données confidentielles : Des informations dont la perte, le vol, la destruction, l'altération ou l'accès par des personnes non autorisées pourrait causer un préjudice important pour l'entreprise. Il s'agit d'informations qui ont un caractère secret, qui sont destinées à être partagées par un groupe limité de personnes. Il peut s'agir d'informations techniques, commerciales, financières, stratégiques, organisationnelles…

données sensibles : Des informations dont la perte, le vol, la destruction, l'altération, l'accès par des personnes non autorisées pourrait causer un préjudice important pour un tiers.

intégrité d'un mot de passe : Garantie de la confidentialité et de la non divulgation d'un mot de passe.

ordinateur hybride (synonyme : tablette hybride) : Equipement informatique pouvant être utilisé en tant que tablette tactile ou en tant qu'ordinateur portable.

service informatique : Ensemble des personnes en charge de l'exploitation, l'installation et la maintenance des Systèmes d'Information dans l'Entreprise.

Système d'Information : Ensemble organisé de ressources (matériels, logiciels, données et procédures) qui permet de traiter, stocker, présenter, détruire et diffuser de l'information, quelle que soit sa forme (électronique, imprimée, vocale…).

Utilisateur : Toute personne autorisée à accéder aux ressources du Système d'Information de l'Entreprise et à les utiliser, quel que soit son statut (notamment salarié, personnel intérimaire, stagiaire, consultant ou prestataire) ou sa localisation (au sein ou hors des locaux de l'Entreprise).

« vie privée résiduelle » : Droit au respect de l'intimité de la vie privée du salarié, même pendant ses horaires de travail et sur son lieu de travail.

VPN : Technologie permettant d'établir une connexion sécurisée via Internet entre un équipement informatique (ex. ordinateur portable) et le Système d'Information de l'Entreprise.

1. Objet de la Charte

Le Système d'Information du Groupe Fives et de ses filiales comprend un ensemble de ressources qui sont mises à la disposition de ses Utilisateurs pour l'accomplissement de leurs missions professionnelles.

L'Entreprise définit et met en œuvre les moyens appropriés pour assurer le bon fonctionnement et la sécurité du Système d'Information, en adéquation constante avec l'évolution des technologies et du cadre réglementaire. Ces moyens visent également à couvrir les risques qu'une négligence et / ou mauvaise utilisation des ressources peuvent faire courir à l'Entreprise (ex. pertes financières, atteinte à la réputation, etc.) et à l'Utilisateur.

La présente Charte définit les droits et les devoirs des Utilisateurs du Système d'Information de l'Entreprise. Elle a pour objectifs d'encadrer les usages des ressources mises à disposition, de sensibiliser les Utilisateurs aux risques de sécurité, de préciser les responsabilités de chacun, et d'informer les Utilisateurs sur les contrôles effectués par l'Entreprise.

Cette Charte expose ainsi les principes et règles de sécurité et de bon usage auxquelles se soumet impérativement tout Utilisateur accédant aux ressources du Système d'Information de l'Entreprise, quel que soit l'équipement utilisé. Par ailleurs, elle identifie les contrôles mis en œuvre dans le respect des droits fondamentaux des Utilisateurs.

2. Champ d'application de la Charte

La présente Charte s'applique à l'ensemble des Utilisateurs du Système d'Information de l'Entreprise quel que soit leur statut (salarié, personnel intérimaire, stagiaire, consultant, prestataire) ou leur localisation (au sein ou hors des locaux de l'Entreprise).

Les principes et règles définis par la présente Charte s'appliquent aux données de l'Entreprise, ainsi qu'aux ressources mises à disposition des Utilisateurs par l'Entreprise :

- Les équipements informatiques : postes de travail (ordinateurs fixes, portables, hybrides), photocopieurs, terminaux mobiles et appareils assimilables (smartphones, tablettes numériques, etc.),
- L'accès aux réseaux informatiques de l'Entreprise et à tous les réseaux (publics ou privés) auxquels on accède depuis le réseau de l'entreprise,
- Les applications, les logiciels, les services de communication (messagerie électronique, messagerie instantanée, solutions de transfert de fichiers, etc.),
- Les supports d'information amovibles (clés USB, disque-durs externes, CD-ROM, etc.).

3. Engagement de respect de la Charte et sanctions

Tout Utilisateur du Système d'Information de l'Entreprise s'engage à respecter l'ensemble des principes, règles et obligations tels que figurant dans la présente Charte. A défaut, il engage sa responsabilité personnelle et / ou la responsabilité de la société qui l'emploie (ex. consultant, prestataire…).

L'Utilisateur fautif s'expose à d'éventuelles sanctions de nature disciplinaire, appropriées et proportionnées, telles que celles définies dans le règlement intérieur, ou de nature commerciale, sans préjuger des actions complémentaires pouvant être engagées à son encontre sur le plan civil et pénal.

Ainsi le non-respect de la Charte peut constituer une faute grave passible d'un licenciement.

En cas de doute quant à l'application des règles de la présente Charte, l'Utilisateur contacte le service des Ressources Humaines de l'Entreprise.

4. Conditions générales d'utilisation des ressources

Les ressources du Système d'Information mises à disposition des Utilisateurs sont la propriété de l'Entreprise. L'usage de ces ressources est gouverné par les principes suivants :

UN ACCES INDIVIDUEL

La plupart des ressources du Système d'Information font l'objet d'un contrôle d'accès et des droits d'accès individuels sont donnés par l'Entreprise à chaque Utilisateur. Ces droits sont strictement personnels et ne peuvent en aucun cas être cédés, prêtés ou transmis de quelque façon que ce soit à un tiers interne ou externe à l'Entreprise, même temporairement. L'Entreprise conserve la pleine maîtrise de l'attribution, modification ou révocation des droits d'accès sur l'ensemble de ses ressources.

Chaque Utilisateur dispose d'un (ou de plusieurs) identifiant(s) et mot(s) de passe pour accéder aux données et aux ressources des Systèmes d'Information de l'Entreprise (poste de travail, compte de messagerie, serveurs, applications…). Les mots de passe sont strictement personnels. Ils doivent impérativement rester confidentiels et, à ce titre, ne doivent jamais être dévoilés à un tiers, y compris au sein de l'Entreprise.

L'Utilisateur ne doit pas utiliser les mêmes mots de passe dans la sphère personnelle et professionnelle et choisir un mot de passe différent par système ou application. Les mots de passe doivent respecter les consignes de sécurité de l'Entreprise concernant leur longueur et complexité, et ne pas pouvoir être devinés facilement.

Les mots de passe ne doivent, en aucun cas, être notés, gardés au bureau ou stockés sous quelque forme que ce soit, excepté dans les solutions fournies à cette fin par l'Entreprise (coffre-fort de mots de passe). En cas de doute sur l'intégrité d'un mot de passe, l'utilisateur doit lancer la procédure de réinitialisation dans les meilleurs délais.

Il est précisé que l'usage de ses identifiants est fait sous l'entière responsabilité de l'Utilisateur. Ainsi, toute connexion, transmission ou utilisation de données effectuée à l'aide de ses identifiants sera présumée avoir été réalisée par l'Utilisateur lui-même.

UN USAGE PROFESSIONNEL

L'Utilisateur réserve l'usage des ressources de l'Entreprise à des fins professionnelles. Il est responsable quant à son utilisation des ressources et respecte, en particulier dans ses accès au Système d'Information, les limites de la mission qui lui a été confiée par l'Entreprise.

L'utilisation des ressources à des fins privées est tolérée pour répondre aux nécessités de la vie courante et familiale, notion de « vie privée résiduelle », sous réserve que cet usage :

- N'affecte pas les conditions d'accès, le bon fonctionnement ou la sécurité des services concernés,
- Ne mette pas en cause la productivité de l'Utilisateur dans l'accomplissement de ses missions professionnelles ni celle de ses collègues,
- S'exerce dans les limites de la législation et des règles définies dans la présente Charte ou de la politique de sécurité des Systèmes d'Information de l'Entreprise,
- Ne puisse en aucun cas nuire aux intérêts ni à l'image de l'Entreprise ou bien encore porter un quelconque préjudice à un tiers,

- N’occasionne pas de coûts ou d’investissements supplémentaires (y compris du temps passé par le service informatique).

L’ensemble des données produites, traitées et stockées sur le Système d’Information de l’Entreprise est présumé à caractère professionnel. Le cas échéant, tout élément à caractère privé présent sur le Système d’Information, doit être identifié par l’Utilisateur en y attachant la mention « Privé », ceci afin que les principes de secret de la correspondance et de respect de la vie privée de l’Utilisateur puissent être appliqués par l’Entreprise. L’Utilisateur est informé que l’Entreprise ne garantit pas la sauvegarde de ces données. Les paragraphes suivants spécifient clairement les ressources sur lesquelles des usages à caractère personnel sont tolérés.

UN USAGE LOYAL ET CONFORME

L’usage des ressources de l’Entreprise par l’Utilisateur doit toujours être loyal et adapté à ses missions professionnelles. L’Utilisateur doit donc :

- Respecter la limite de ses droits d’accès sur les ressources,
- S’interdire tout usage excessif des ressources (téléchargements non nécessaires, inutilement volumineux, impressions superflues, etc.),
- Ne pas détourner des ressources pour un usage personnel (hors tolérance mentionnée plus haut),
- Ne se livrer à aucune activité qui serait contraire à la loi ou qui serait contraire aux engagements de l’Entreprise, à sa réputation ou à ses intérêts.

L'utilisation du Système d’Information de l’Entreprise doit s'effectuer dans le respect des droits des personnes, en excluant notamment les atteintes à la vie privée ou au secret des correspondances, les incitations aux crimes et aux délits, les propos à caractère sexiste ou discriminatoire, les diffamations et injures publiques, les dénonciations calomnieuses ainsi que la consultation et la diffusion de contenus manifestement illicites ou pouvant heurter la sensibilité d’une autre personne (contenus violents, obscènes, pornographiques ou d’autre nature potentiellement choquants). Il est par ailleurs strictement interdit d’accéder à des serveurs ou sites internet présentant ces caractéristiques.

L’Utilisateur ne porte pas atteinte aux systèmes informatiques internes ou externes (accès frauduleux, entrave, etc.), ni aux données de ceux-ci (modification, suppression ou introduction frauduleuse). Il se garde de tout acte constitutif de contrefaçon. Il s’interdit de contrevenir, d’une quelconque manière, aux droits de propriété industrielle ou intellectuelle (ex : installation de logiciels sans licences…).

L’Utilisateur ne doit pas, à titre personnel, prêter, vendre ou céder à des tiers, les logiciels, licences, programmes d’installation et outils fournis par l’Entreprise, et ce y compris les logiciels développés spécifiquement pour les besoins de l’Entreprise.

L’Utilisateur ne doit pas prêter (y compris dans la sphère familiale ou amicale), louer, vendre ou céder à des tiers, les équipements fournis par l’Entreprise.

Il est interdit à tout Utilisateur de faire transiter par, ou de conserver sur, les ressources de l’Entreprise ou mises à sa disposition par l’Entreprise (équipements, serveurs, services de messagerie, solutions Cloud…), des données confidentielles, dont un tiers pourrait revendiquer la propriété et qui ne seraient pas par ailleurs accessibles de manière publique. De même, lorsqu’un Utilisateur quitte l’Entreprise, il ne peut prendre copie des données de l’Entreprise.

UN DEVOIR DE PROTECTION PHYSIQUE DES EQUIPEMENTS

L'Utilisateur est responsable de la sécurité physique des équipements qui lui sont confiés par l'Entreprise dans le cadre de sa mission. Aussi il veille à en avoir une utilisation respectueuse (ex. éviter les chocs, ne pas manipuler de liquides à proximité, placer le matériel dans un lieu sûr et stable) et il s'engage à prendre les mesures adaptées pour réduire les risques de casse, perte ou vol. Ainsi, lors de ses déplacements, l'Utilisateur ne laisse jamais d'équipements sans surveillance dans un lieu public.

L'Utilisateur prévient impérativement et dans les meilleurs délais le service informatique de l'Entreprise en cas de perte ou de vol (supposé ou avéré) d'un poste de travail, d'un terminal mobile et / ou de la carte SIM, et ce afin que les mesures nécessaires à la protection du Système d'Information de l'Entreprise soient mises en œuvre.

Dans le cas d'une disparition intervenue hors des locaux de l'Entreprise, dans la mesure du possible, l'Utilisateur dépose une plainte auprès des autorités compétentes dans les meilleurs délais compatibles avec sa mission, puis adresse une copie de cette plainte au service des Ressources Humaines de l'Entreprise.

UN DEVOIR DE VIGILANCE

La Sécurité du Système d'Information de l'Entreprise passe par la vigilance de tous. A cet effet, l'Utilisateur signale dans les meilleurs délais au service informatique tout incident de sécurité potentiel qu'il constate sur l'un de ses équipements (dysfonctionnements, lenteurs, comportements inhabituels) ou toute situation à risque sur ses données.

L'Utilisateur prend connaissance et tient compte des messages de sensibilisation divulgués par l'Entreprise ou par le Groupe sur les risques liés à la sécurité de l'information et des systèmes d'information. Il participe aux présentations et suit les formations obligatoires organisées sur ces sujets par son Entreprise ou par le Groupe.

5. Règles de sécurité et de bon usage des ressources

5.1. Postes de travail

L'Entreprise met à disposition de ses Utilisateurs des postes de travail (ordinateurs fixes, portables ou hybrides) destinés à l'accomplissement de leur mission professionnelle. Ces postes de travail sont paramétrés et administrés à cet effet par le service informatique de l'Entreprise.

Un usage, à titre privé, de ces ressources est toléré dans les limites définies au chapitre précédent. Lorsque des données stockées sur ces postes de travail relèvent de sa « vie privée résiduelle », l'Utilisateur les place dans un dossier ou répertoire portant explicitement la mention « Privé ».

REGLES RELATIVES A LA SECURITE ET LA PROTECTION DES POSTES DE TRAVAIL

L'Utilisateur respecte les règles de protection physique des équipements définies au chapitre précédent.

L'Utilisateur protège l'accès à son poste de travail en respectant les règles de sécurité relatives aux mots de passe et en verrouillant systématiquement sa session dès qu'il s'absente, même temporairement, de son poste de travail.

L'Utilisateur s'engage à ne pas installer sur son poste de travail des logiciels autres que ceux fournis par l'Entreprise sauf dérogation préalablement obtenue du service informatique. Lorsque les activités métiers requièrent l'utilisation d'un logiciel spécifique non fourni et / ou installé sur son poste de travail, l'utilisateur en fait la demande conformément aux procédures en vigueur dans l'Entreprise. Le service informatique peut ainsi s'assurer du respect de la législation en matière de propriété intellectuelle, et le cas échéant s'acquitter de droits d'usage et de licences des logiciels.

L'Utilisateur s'engage à ne pas contourner les moyens de sécurisation ou de filtrage des ressources mis en place par l'Entreprise (ex. plateformes d'accès sécurisé, anti-virus, proxy), ou nuire à leur bon fonctionnement. Il est rappelé que seul le service informatique de l'Entreprise est autorisé à effectuer des opérations de maintenance sur les équipements informatiques.

L'Utilisateur n'utilise pas d'outil de chiffrement des données autre que ceux fournis et / ou autorisés par l'Entreprise, de sorte que les données professionnelles demeurent accessibles en l'absence de l'Utilisateur pour répondre aux besoins de continuité d'activité ou de réquisition judiciaire.

L'Utilisateur s'interdit de connecter tout équipement personnel au réseau interne de l'Entreprise.

REGLES RELATIVES A L'UTILISATION DE SUPPORTS AMOVIBLES

L'Utilisateur doit éviter, lorsque cela est possible, la connexion de supports amovibles sur son poste de travail, en privilégiant l'utilisation des solutions de transfert de données mises à sa disposition par l'Entreprise. Lorsque cela est strictement nécessaire, pour répondre à un besoin professionnel de transfert ponctuel de données, l'Utilisateur doit s'assurer que le support utilisé ne contient pas de virus (avec éventuellement l'aide du service informatique).

L'Utilisateur ne doit en aucun cas connecter à son poste de travail un support amovible dont l'origine est inconnue ou estimée à risque.

REGLES RELATIVES A L'UTILISATION DES POSTES DE TRAVAIL EN SITUATION DE MOBILITE

Comme évoqué au chapitre précédent, l'Utilisateur adopte les bons comportements pour limiter le risque de perte ou de vol de ses équipements en dehors des locaux de l'Entreprise (transports en commun, hôtels / restaurants, sites professionnels tiers…).

Il fait preuve de vigilance pour limiter le risque de divulgation d'informations confidentielles lors de ses déplacements. Il utilise un filtre de confidentialité lorsqu'il utilise son ordinateur portable dans un lieu public (en particulier dans les transports en commun…).

Il ne stocke jamais d'informations stratégiques sur des équipements portables non chiffrés.

Enfin il prend connaissance des consignes de l'Entreprise relatives aux déplacements professionnels à l'étranger et les applique.

REGLES RELATIVES A LA SAUVEGARDE DES DONNEES

L'Utilisateur veille à ce que toutes les données professionnelles stockées sur son poste de travail soient sauvegardées sur une ressource réseau de l'Entreprise, ou à défaut une solution Cloud mise en place par l'Entreprise. Les données personnelles de l'Utilisateur doivent être exclues de ces sauvegardes. Lorsque cela est possible, l'Utilisateur doit éviter le stockage de documents en local sur son poste de travail, et privilégier l'utilisation des répertoires réseaux mis à disposition par l'Entreprise. Il convient de rappeler que l'Entreprise met en œuvre les

mesures nécessaires pour sauvegarder les données stockées sur les ressources réseaux de l'Entreprise.

5.2. Internet

L'Entreprise met à disposition de ses Utilisateurs un accès Internet destiné à un usage professionnel. Il est paramétré et administré à cet effet.

Un usage, à titre privé, de l'accès Internet mis à disposition par l'Entreprise est toléré dans les limites définies au chapitre précédent.

REGLES RELATIVES A LA SECURITE DES MOYENS DE CONNEXION

L'Utilisateur doit obligatoirement utiliser en l'état les moyens de connexion à Internet fournis par l'Entreprise. A ce titre, l'Utilisateur s'interdit de modifier les paramètres de sécurité ou de contourner les restrictions mises en place par l'Entreprise, et utilise impérativement les navigateurs Internet installés par le service informatique de l'Entreprise.

Dans le cas d'une connexion hors des locaux de l'Entreprise, l'Utilisateur privilégie l'utilisation des moyens mis à disposition par l'Entreprise (connexion à la data mobile…, connexion sécurisée VPN…) et évite l'utilisation des points d'accès Wifi publics.

REGLES RELATIVES A L'UTILISATION DE L'ACCES INTERNET

Comme évoqué au chapitre précédent, l'Utilisateur s'engage à ne pas utiliser l'accès Internet mis à disposition par l'Entreprise pour toute activité (consultation de site, transmission / téléchargement de documents…) comportant des éléments manifestement illicites ou non conformes aux règles de l'Entreprise.

L'Utilisateur doit impérativement limiter toute activité engendrant un large trafic (téléchargements volumineux, radios en ligne, vidéos en ligne, etc.) à des fins strictement professionnelles. Même dans ce cadre, il prend soin de les limiter au strict nécessaire.

Pour des impératifs de sécurité, de disponibilité et de performance des ressources, l'Entreprise se réserve le droit de filtrer, limiter et contrôler l'accès Internet fourni aux Utilisateurs. L'Utilisateur peut adresser au service informatique une demande de levée partielle de ces mesures. L'Entreprise se réserve le droit de donner une suite favorable ou non à cette demande.

REGLES SPECIFIQUES RELATIVES A L'UTILISATION DES BLOGS ET DES RESEAUX SOCIAUX

L'Utilisateur doit impérativement respecter la confidentialité des données de l'Entreprise, et ne pas publier d'information confidentielle ou sensible sur les blogs ou réseaux sociaux. De manière générale, l'Utilisateur doit faire preuve d'une grande vigilance afin de s'assurer que la communication sur ces médias ne soit pas, directement ou indirectement, préjudiciable aux intérêts et à la réputation de l'Entreprise et du Groupe.

L'Utilisateur n'est pas autorisé à communiquer au nom de l'Entreprise sans accord préalable formel de la Direction de l'Entreprise.

Pour les communications professionnelles sur les blogs ou réseaux sociaux, l'Utilisateur s'interdit d'usurper ou d'emprunter l'identité d'un tiers, il utilise sa propre identité.

5.3. Intranet, applications et serveurs internes

L'accès à l'Intranet, aux applications et aux serveurs internes de l'Entreprise est mis à disposition des Utilisateurs pour un usage professionnel. Il est paramétré et administré à cet effet.

Pour des raisons de performance et de maîtrise du réseau, l'usage à titre privé de ces ressources n'est pas autorisé.

5.4. Réseau Social d'Entreprise / de Groupe

L'Utilisateur dispose d'un accès au Réseau Social d'Entreprise du Groupe Fives. Cette solution lui permet d'échanger avec les collaborateurs de son Entreprise ou avec tous les collaborateurs du Groupe Fives.

La solution ne faisant pas l'objet d'un système centralisé de modération de contenu, l'Utilisateur se doit de respecter les règles décrites dans la Charte d'Utilisation du Réseau Social du Groupe Fives.

Tout Utilisateur peut être à l'initiative de la création de groupes de discussion sur le Réseau Social d'Entreprise ; il s'engage à modérer les échanges effectués dans ses groupes.

L'Utilisateur doit absolument s'assurer que les informations qu'il diffuse peuvent être communiquées à l'audience concernée, que le groupe soit public ou privé.

Les groupes privés doivent être réservés aux communautés abordant des thèmes spécifiques pour lesquels une communication globale n'est ni utile, ni nécessaire, ni souhaitable.

5.5. Messageries

L'Entreprise met à disposition de ses Utilisateurs une messagerie électronique, et le cas échéant une messagerie instantanée, destinées à un usage professionnel. Ces services sont paramétrés et administrés à cet effet.

Un usage, à titre privé, des services de messageries mis à disposition par l'Entreprise est toléré dans les limites définies au chapitre précédent (messages relevant de la « vie privée résiduelle » de l'Utilisateur). L'application par l'Entreprise des principes de secret des correspondances et de respect de la vie privée nécessite que l'Utilisateur respecte les règles suivantes : la mention « Privé » doit systématiquement figurer au début de l'objet du message, le tiers destinataire doit être informé de cet usage, toute signature identifiant l'Entreprise (notamment en fin de message) doit être supprimée et enfin les messages privés doivent être rangés dans un répertoire dédié de la messagerie portant la mention « Privé ».

REGLES RELATIVES A LA SECURITE DES SERVICES DE MESSAGERIES

L'Utilisateur doit obligatoirement utiliser en l'état les services de messagerie installés et configurés par l'Entreprise. A ce titre, l'Utilisateur s'interdit de modifier les paramètres de sécurité, et utilise impérativement le logiciel de messagerie installé par le service informatique de l'Entreprise.

Il s'engage à ne pas utiliser, pour ses usages professionnels, de services de messagerie ou de partage de données autres que ceux mis à disposition par l'Entreprise. Il est ainsi interdit d'utiliser à des fins professionnelles une messagerie personnelle (Gmail, Yahoo…) ou un service de stockage ou de transfert de fichiers grand public (Google Drive, WeTransfer…).

L'Utilisateur s'interdit également de transférer des messages de sa messagerie professionnelle vers sa messagerie personnelle.

L'Utilisateur n'utilise pas son adresse de messagerie professionnelle afin de créer des comptes dans des applications ou sur des sites pour un usage non professionnel.

REGLES RELATIVES A L'USAGE DES SERVICES DE MESSAGERIES

Pour la rédaction de messages électroniques, l'Utilisateur adopte des formulations adaptées et contrôle systématiquement la liste des destinataires avant envoi.

Il s'engage à ne pas utiliser les services de messagerie mis à disposition par l'Entreprise pour envoyer ou faire suivre des messages comportant des éléments manifestement illicites ou non conformes aux règles de l'Entreprise.

Il ne doit pas procéder à des envois en nombre de messages à destination d'adresses externes, sauf accord préalable formel du service informatique de l'Entreprise qui proposera, le cas échéant, des solutions adaptées.

L'Entreprise se réserve le droit, pour des impératifs de sécurité, de disponibilité et de performance des ressources, de limiter la taille maximum des messages, des boîtes aux lettres et de certains types de fichiers attachés. L'Entreprise met à disposition des Utilisateurs des solutions spécifiques, autres que la messagerie, pour gérer les transferts de documents volumineux.

REGLES RELATIVES A LA PROTECTION CONTRE L'HAMEÇONNAGE ET LA FRAUDE

L'Utilisateur doit éviter, autant que faire se peut, de publier son adresse électronique sur Internet.

Il doit faire preuve d'une vigilance accrue en cas de réception d'un message inhabituel ou douteux en provenance d'un expéditeur inconnu, présentant une syntaxe approximative, contenant des liens vers des sites et / ou des pièces jointes non sollicités, ou demandant d'effectuer des actions inhabituelles. Lorsque l'Utilisateur pense avoir reçu un tel message (ou s'il a le moindre doute sur un message), il n'y répond pas et le signale immédiatement au service informatique de l'Entreprise, sans tenter d'accéder aux liens contenus dans le message ou d'ouvrir les pièces jointes associées.

Il ne doit cliquer sur un lien hypertexte contenu dans un message que lorsqu'il estime avoir « toute confiance » dans l'expéditeur et seulement après avoir vérifié la syntaxe du lien hypertexte.

En raison des risques d'usurpation d'une adresse de messagerie, l'Utilisateur doit faire preuve de discernement en cas de réception d'un message électronique qui semble provenir d'un responsable ou d'un tiers connu, lui demandant d'effectuer des actions inhabituelles ou non-conformes aux procédures internes. Dans ce cas, il doit vérifier verbalement auprès de cette personne le bienfondé de l'action (échange téléphonique, rencontre physique...).

REGLES RELATIVES A L'ENVOI DE DONNEES CONFIDENTIELLES OU SENSIBLES PAR COURRIEL

Il convient de rappeler qu'il est impossible de garantir la confidentialité des échanges effectués par courriel. En conséquence il convient d'éviter d'échanger des informations confidentielles ou sensibles par messagerie électronique sans avoir recours à une solution de chiffrement fournie par l'Entreprise.

5.6. Terminaux mobiles

L'Entreprise met à disposition des Utilisateurs, lorsque leurs missions professionnelles l'exigent, un terminal mobile (téléphone mobile, smartphone, tablette numérique…) et une carte SIM avec abonnement pour l'exercice de ces missions. Dans ce cadre, l'Entreprise demeure propriétaire du terminal mobile mis à disposition et titulaire de l'abonnement attaché à la carte SIM.

L'utilisation d'un terminal mobile personnel pour l'accomplissement des missions professionnelles est interdite, sauf autorisation formelle de la Direction de l'Entreprise. En conséquence l'installation d'une messagerie professionnelle sur un terminal mobile personnel est strictement interdite sauf dérogation expresse de la Direction.

REGLES RELATIVES A LA SECURITE DES TERMINAUX MOBILES

L'Utilisateur respecte les règles de protection physique des équipements définies au chapitre précédent.

Il ne modifie pas les paramètres de sécurité des terminaux mobiles configurés par l'Entreprise. Il s'interdit notamment de débrider ou pirater le terminal mobile.

Il configure impérativement sur son terminal mobile un code de verrouillage non trivial, et il utilise systématiquement la fonctionnalité de verrouillage automatique après une courte période d'inactivité.

Il ne doit pas connecter son terminal mobile à des dispositifs ou des équipements sans valider préalablement leur niveau de sécurité (ex. ordinateur d'un tiers, borne d'alimentation autre qu'une prise électrique – i.e. une prise USB ou un dock dans les hôtels ou espaces publics…).

REGLES RELATIVES A LA SAUVEGARDE ET LA SYNCHRONISATION DES DONNEES

L'Utilisateur doit veiller à sauvegarder périodiquement et de façon sécurisée les données importantes stockées sur son terminal mobile.

Il s'interdit de sauvegarder ou de synchroniser des données sur des ressources non mises à disposition par l'Entreprise (ex. Google Drive …).

REGLES RELATIVES A L'UTILISATION DES MOYENS DE CONNEXION

En déplacement à l'étranger l'Utilisateur prend soin de limiter les coûts. En particulier il maîtrise la consommation de données en désactivant « les données mobiles » paramétrées par défaut et en gérant ponctuellement leur réactivation.

Il doit faire preuve d'une vigilance particulière face aux risques de sécurité spécifiques liés à l'utilisation de terminaux mobiles, notamment il ne valide aucune demande de mise en relation qu'il n'a pas initiée ou planifiée, il ne répond pas à un SMS / MMS inhabituel ou douteux, et ne scanne pas de flash code ou de QR code affichés dans des lieux publics ou donnés par des sources non sûres.

REGLES RELATIVES AU TELECHARGEMENT ET A L'INSTALLATION D'APPLICATIONS

L'Utilisateur doit limiter le téléchargement d'applications à des besoins strictement professionnels.

L'Utilisateur ne télécharge des applications qu'après en avoir vérifié la réputation et uniquement depuis des stores de confiance. Il contrôle (et éventuellement ajuste) les droits d'accès demandés par l'application lors de son installation (ne pas autoriser les accès aux données du téléphone comme les contacts, les photographies, la géolocalisation… quand ce n'est pas justifié et lorsque c'est possible).

Il ne doit pas utiliser de systèmes de messagerie instantanée autres que ceux fournis par l'Entreprise pour échanger des données professionnelles confidentielles ou sensibles (par exemple WhatsApp, Viber, WeChat ou équivalent…).

Il se doit d'être vigilant dans l'utilisation d'une application générant des coûts spécifiques (abonnement, paiement à l'acte, téléchargement de contenus payants) dans le cas où ces coûts seraient imputables sur la facture téléphonique professionnelle.

REGLES RELATIVES A L'UTILISATION DES TERMINAUX MOBILES

L'Utilisateur est responsable de l'utilisation des terminaux mobiles mis à sa disposition par l'Entreprise. Ainsi, l'Entreprise ne saurait être tenue pour responsable des contenus illégaux et / ou illicites qui pourraient être stockés sur le terminal et de tout acte malveillant ou frauduleux réalisé au moyen de la carte SIM.

Il s'engage à avoir un usage raisonnable de l'abonnement attaché à la carte SIM. Afin d'ajuster au mieux les options liées à l'abonnement téléphonique professionnel attaché au terminal, l'Entreprise prend connaissance chaque mois des volumes et coûts de ses consommations.

Par ailleurs l'Utilisateur est invité à contacter le service informatique de l'Entreprise, lorsque cela est nécessaire, pour ajuster les caractéristiques de son abonnement téléphonique aux besoins liés à son activité professionnelle.

REGLES RELATIVES AUX CONTROLES REALISES PAR L'ENTREPRISE

L'Entreprise s'engage à respecter la vie privée des Utilisateurs et à ne pas utiliser les données à caractère non professionnel identifiées comme telles dont elle pourrait avoir connaissance.

L'Utilisateur est informé que le service informatique peut vérifier ou mettre à jour les paramètres de sécurité ou les applications et effacer à distance les données en cas de perte ou de vol de tout terminal connecté aux Systèmes d'Information de l'Entreprise.

L'Entreprise se réserve le droit de mettre un terme à la mise à disposition du terminal mobile professionnel et de l'abonnement professionnel en cas de négligences ou de malveillances constatées dans l'utilisation du terminal ou de la carte SIM fournie.

6. Traitement de données à caractère personnel

RESPONSABILITE ET DEVOIRS DES UTILISATEURS

Un Utilisateur qui reçoit ou accède à des données à caractère personnel, qu'il s'agisse de données relatives aux collaborateurs de l'Entreprise ou à des tiers (clients, partenaires, candidats…), s'engage à respecter strictement la réglementation applicable, la Politique de protection des données personnelles de l'Entreprise ainsi que les procédures associées au traitement de ces données.

DROITS DES UTILISATEURS

Conformément à la réglementation applicable en matière de données à caractère personnel les Utilisateurs sont informés qu'ils disposent d'un certain nombre de droits relatifs aux informations personnelles les concernant. Ces droits sont décrits dans la Politique spécifique de protection des données personnelles des collaborateurs.

L'Utilisateur peut exercer ces droits en contactant la personne désignée par l'Entreprise, ou à défaut le service des Ressources Humaines de l'Entreprise.

7. Contrôle des ressources

Conformément à la loi, la responsabilité juridique de l'Entreprise peut être engagée en raison de l'utilisation faite par les Utilisateurs des ressources du Système d'Information de l'Entreprise. L'Entreprise se réserve donc le droit d'analyser, de limiter et de contrôler l'utilisation des ressources matérielles et logicielles ainsi que les échanges effectués via ses Systèmes d'Information.

OBJET ET ENCADREMENT DES CONTROLES REALISES PAR L'ENTREPRISE

Les contrôles mis en œuvre par l'Entreprise sont réalisés par les Administrateurs informatiques dans l'objectif de garantir le bon fonctionnement technique et la sécurité du Système d'Information, et de préserver les intérêts de l'Entreprise.

Les contrôles sont réalisés dans le respect de la législation applicable et dans le respect de la vie privée.

Les contrôles sont réalisés exclusivement par les membres habilités du service informatique de l'Entreprise qui garderont confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion.

OPERATIONS RECURRENTES DE CONTROLE SUR LES JOURNAUX D'EVENEMENTS

L'Entreprise met en œuvre différents dispositifs de contrôle de l'utilisation des ressources du Système d'Information. Ces dispositifs génèrent des journaux conservant les traces de certaines actions des Utilisateurs. La liste des dispositifs de contrôle mis en place, ainsi que les éléments journalisés et leur durée de conservation, sont communiquées aux utilisateurs. Le service informatique de l'Entreprise réalise des opérations récurrentes de contrôle portant sur ces journaux.

OPERATIONS PONCTUELLES DE CONTROLE SUR LES DONNEES

L'Entreprise peut à tout moment et en dehors de la présence des Utilisateurs, opérer tout contrôle sur les données présumées à caractère professionnel, qu'il s'agisse par exemple de la messagerie électronique ou des fichiers enregistrés. L'accès aux données est réalisé par les membres habilités du service informatique de l'Entreprise sur demande formelle de certaines personnes de la Direction de l'Entreprise (DG, DRH, DAF).

Dans le cas de fichiers identifiés comme étant de nature privée conformément aux règles précisées dans la présente Charte, les Administrateurs informatiques en charge des opérations de contrôle peuvent néanmoins procéder à des contrôles sur la taille, le volume et la nature des fichiers, et ce sans accéder aux données. L'Entreprise ne peut accéder à ces

données qu'en présence de l'Utilisateur ou lorsque celui-ci a été dûment invité à être présent par tout moyen approprié.

En cas de risque ou évènement particulier présentant à la fois un caractère d'urgence et de gravité certain, l'Entreprise peut néanmoins accéder aux fichiers identifiés comme étant de nature privée sans la présence ou la convocation de l'Utilisateur.

En cas d'accès à des données se rapportant de manière évidente à la vie privée d'un Utilisateur mais non signalées comme telles par l'intéressé, aucune faute ne peut être retenue à l'encontre de l'Entreprise et / ou de l'Administrateur informatique en charge des opérations de contrôle. Dans ce cas, et à l'exception d'une réquisition judiciaire, l'Administrateur informatique applique le droit au respect de la vie privée de l'Utilisateur conformément aux principes définis dans la présente Charte.

ACTIONS SUITE AUX CONTROLES

Dans le cas de circonstances graves d'utilisations illégales, non autorisées ou remettant en cause le bon fonctionnement des Systèmes d'Information, la sécurité ou les intérêts de l'Entreprise, les membres du service informatique de l'Entreprise pourront mettre en œuvre les actions de protection adaptées ainsi que les corrections nécessaires jusqu'au retour à la normale. Ils en informeront la Direction de l'Entreprise.

8. Entrée en vigueur de la Charte

La présente Charte, annexée au règlement intérieur de l'Entreprise, a été soumise pour avis au CSE, et transmise à l'autorité administrative compétente.

Elle est déposée au secrétariat du greffe du Conseil des Prud'hommes compétent.

Elle est affichée sur les tableaux réservés à l'information du personnel et elle entrera en vigueur un mois après son affichage. Elle sera également disponible sur l'Intranet de l'Entreprise.

Elle entrera en vigueur le 1 septembre 2019.

Les modifications et adjonctions apportées à la présente Charte feront l'objet des mêmes procédures de consultation, de publicité et de dépôt.

Fait à Nancy, le 23 mai 2019.

Jean-Jacques DEPUYDT

Président

DocuSigned by:

556E2CCA758D478...