NP AKADIN – EVOBAT

CHARTE INFORMATIQUE

Table des matières

I Description

La présente charte a été établie afin de définir concrètement l'ensemble des règles d'utilisation et d'usages des ressources informatiques mise à disposition des collaborateurs du groupe NP AKADIN.

L'objectif commun et partagé de l'établissement de ces règles vise à mettre en place une sécurité coordonnée, un usage propre des ressources et des règles de bonne conduite de l'utilisateur afin de :

- Protéger au maximum l'intégrité des données de l'entreprise ;
- Assurer la confidentialité des données ;
- Protéger les informations contre le piratage, les vols, effacements ou pertes ;
- Assurer la cybersécurité du système d'information mise en place ;
- Optimiser l'utilisation des ressources informatiques ;
- Déterminer les limites d'utilisation des ressources informatiques pour éviter les pratiques abusives ou négligentes ;
- Eviter les mauvaises manipulations assurant ainsi la continuité des services et la disponibilité maximum des ressources informatiques pour la production ;
- Définir la politique de gestion et d'utilisation des ressources informatiques par le personnel d'encadrement ;
- Définir les modalités d'utilisation d'internet et de ses dérivées ;
- Définir les règles disciplinaires à appliquer en cas de non-respect de la présente charte.

La charte sur validation du secrétaire générale est appliquée et demeure en vigueur jusqu'à publication d'une mise à jour ou sur nouvel ordre. Elle reste un outil essentiel pour une utilisation responsable et sécurisée des ressources informatiques de l'entreprise.

Afin de tenir compte du contexte juridique et technologique en rapide évolution, la charte sera réactualisée régulièrement et les utilisateurs en seront informés. La DSI organisera également des formations adaptées pour fournir des informations complémentaires sur l'application de la charte.

Tout collaborateur se doit dans l'obligation de lire et signer avec la mention « Lu et approuvé » la présente charte afin d'accéder pleinement aux ressources informatiques.

II ARTICLE 1 : INTERNET ET MESSAGERIE ELECTRONIQUE

L'utilisation d'Internet et de la messagerie électronique est autorisée dans le cadre de l'activité professionnelle. Toutefois, l'accès à certains sites peut être bloqué par mesure de sécurité ou pour éviter toute utilisation abusive. Les utilisateurs sont tenus de respecter les règles de bonne conduite et de ne pas consulter de sites ou de diffuser des informations contraires aux bonnes mœurs ou à la législation en vigueur. Tout contenu ou message inapproprié doit être signalé immédiatement le secrétaire général et au service informatique.

II.1 INTERNET

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder sont destinés l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, modem, borne d'accès sans fil…) sur le réseau sont soumises à autorisation du responsable et aux règles de sécurité de NP AKADIN. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée.

L'entité peut en outre prévoir des restrictions d'accès spécifiques à son organisation (certificats électroniques, cartes à puce d'accès ou d'authentification, filtrage d'accès sécurisé…).

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

- De communiquer à des tiers des informations techniques concernant son matériel ;
- De connecter un micro à Internet via un modem (sauf autorisation spécifique) ;
- De diffuser des informations sur l'entreprise via des sites Internet ;
- De participer à des forums (même professionnels) ;
- De participer à des conversations en ligne (« chat »).

II.1.1 Utilisation d'Internet à des fins privées

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

Les limites du raisonnables se définissent comme suit :

- Ne pas utiliser la connexion pour le téléchargement (films, séries, jeux, logiciels) ;
- Ne pas utiliser la connexion pour le streaming ;
- Utiliser uniquement la connexion pour contacter des personnes proches pour des cas d'urgences ou motif importants (santé, enfants/écoles, accidents, évènements tragiques) ;

II.1.2 Contrôles de l'usage

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

- Les durées des connexions (précisez : de façon globale / par service / par utilisateur) ;
- Les sites les plus visités (précisez : de façon globale / par service) ;
- Les accès sur les réseaux sociaux et les sites vidéoludiques (liste en annexe) ;
- Les sites à titre ou caractère sexuels (liste en annexe);
- Les sites dangereux (blackmarket, BOT spy, sites de rencontres, …).

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel et le secrétaire général.

II.2 MESSAGERIE ELECTRONIQUE

Les serveurs mails seront hébergés chez MICROSOFT avec l'offre EXCHANGE PLAN 1, le serveur messagerie utilisés par le groupe sera MICROSOFT OFFICE OUTLOOK. L'usage d'un autre client de messagerie est interdit car l'organisation, les rendez-vous, meetings et les plannings seront basés sur le calendrier partagé OUTLOOK.

II.2.1 Fonctionnement

- Il est interdit de supprimer un mail, chaque mail représente un élément important de la traçabilité des activités du groupe NP AKADIN, supprimer un email peut être considérer comme un acte de nuisance au groupe et comme une faute professionnelle ;
- Le collaborateur doit impérativement classer ses mails dans des dossiers et appliquer des règles de gestion sur les adresses emails importants, le classement doit être effectué de manière cohérente et ordonnée afin que les responsables hiérarchiques puissent retrouver facilement les emails importants ;
- Pour tout rendez-vous, chaque collaborateur doit utiliser le système de calendrier OUTLOOK afin que ses supérieurs hiérarchiques puissent avoir une parfaite visibilité du planning de travail ;

- Pour une parfaite maitrise de l'outil de travail OUTLOOK, chaque collaborateur est libre de poser des questions à la DSI qui se chargera d'apporter les explications nécessaires pour le bon usage de l'outil ;
- Un archivage automatique des mails sera effectué tous les 6 mois ;
- Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système de la sauvegarde des fichiers et courriers électroniques de l'utilisateur.

II.2.2 Interdiction et barrière

- Envoi d'information stratégique, sauf crypter au préalable par la DSI.
- S'inscrire sur des sites et services illégaux, peu fiables, peu recommandables ou suspects, ou suivre des liens suspects vous invitant à des jeux de loteries pouvant conduire aux vols de vos informations d'authentification.
- Envoyer du contenu marketing ou des e-mails de prospection non autorisés.
- S'inscrire aux services d'un concurrent sans y être autorisé.
- Envoyer des messages et des contenus insultants ou discriminatoires.
- Envoyer des spams intentionnellement à d'autres personnes, y compris leurs collègues.
- Utiliser des services d'un site web spécialisé dans la messagerie.
- Envoyer de messages sexistes, racistes ou autres ;
- Envoyer de contenu diffamatoire ;
- Envoyer de contenu protégé par les droits d'auteur ;
- Envoyer de liens vers du contenu inapproprié.

II.2.3 Conditions d'utilisations

- Toute utilisation du courrier électronique doit être conforme aux chartes de la société en matière de conduite éthique et de sécurité des données professionnelles.
- Ne pas cliquer ou télécharger des pièces jointes d'un mail suspect ou inhabituel (nom de domaine inconnu ou bizarre), toujours aviser la DSI en cas de détection ;
- Toute utilisation de la messagerie électronique doit être conforme aux pratiques commerciales appropriées et pertinentes pour les tâches professionnelles.
- Les adresses électroniques ou les systèmes de la société ne doivent pas être utilisés pour créer, distribuer ou accéder à tout matériel offensant ou illégal, y compris, mais sans s'y limiter, le matériel contenant des commentaires offensants sur le sexe, la race, l'âge, l'orientation sexuelle ou les croyances religieuses.
- Tout matériel offensant reçu par courrier électronique doit être signalé sans délai au département informatique et aux ressources humaines.

- L'utilisation des adresses électroniques et des systèmes appartenant à l'entreprise à des fins personnelles doit être limitée à un usage minimal et occasionnel, minimal et occasionnel se définissent par une utilisation personnelle justifiée par un cas d'urgence ou motif très importants (santé, enfants/écoles, accidents, évènements tragiques) ;
- Il est interdit d'utiliser des adresses électroniques ou des systèmes appartenant à l'entreprise à des fins personnelles ou liées à des affaires ne faisant pas partie des activités de l'entreprise.
- Les e-mails reçus aux adresses électroniques de la société ne peuvent être automatiquement transférés à des adresses électroniques qui ne sont pas détenues ou exploitées par la société.
- Les adresses électroniques individuelles transmises à des adresses électroniques qui ne sont pas détenues ou exploitées par la société ne doivent pas contenir d'informations sensibles ou confidentielles.
- La création ou la transmission de blagues à partir d'adresses électroniques ou de systèmes de la société est interdite.
- Le groupe NP AKADIN peut se réserve le droit de surveiller et enregistrer tous les messages électroniques reçus ou envoyés par des adresses électroniques ou des systèmes détenus ou exploités par la société.
- Mettre une sécurité de double authentification sur les adresses emails, en cas de la perte de la deuxième authentification aviser la DSI pour l'utilisation d'un code de récupération ;

III ARTICLE 2 : PROTECTION DES DONNEES ET COMPTES UTILISATEURS

III.1 Confidentialité et protection des données

La protection des données est une priorité de l'entreprise. Les utilisateurs sont tenus de respecter les règles de confidentialité et de ne pas divulguer des informations confidentielles à des tiers, ni de procéder à des copies, déplacement, externalisation des données de l'entreprise. Les mots de passe doivent être régulièrement renouvelés tous les 6 mois et ne doivent pas être partagés, affichés, ou facilement accessibles. Les fichiers doivent être sauvegardés sur le serveur de l'entreprise, les périphériques USB personnels sont bloqués. Les données stockées sur les disques durs des postes informatiques ne sont pas sauvegardées.

Chaque collaborateur aura un login et mot de passe enregistrés dans l'annuaire ACTIVE DIRECTORY du groupe. Ces informations sont extrêmement confidentielles et ne doivent être communiquées à une tierce personne.

III.2 Sécuriser l'accès au compte

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Il doit choisir des mots de passe sûrs, en respectant les règles fixées par les administrateurs. Un bon mot de passe doit contenir au moins 8 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux. Eviter de mettre dans les mots de passes des informations personnelles ou nom de compte (date de naissance, nom d'un proche, nom enfant … etc ...).

Il doit les garder secrets et ne pas les communiquer à des tiers. Toutefois, en cas d'absence, l'utilisateur pourra — à la demande de son responsable hiérarchique et si l'accès à un fichier, dossier, message professionnel est indispensable au bon fonctionnement du service — être tenu de communiquer son mot de passe audit responsable hiérarchique après validation du secrétaire général. Il appartiendra à l'agent de modifier son mot de passe à son retour.

Chaque mot de passe sera réinitialisé automatiquement tous les 6 mois et le collaborateur sera invité à changer de mot de passe afin de renforcer la sécurité de son compte. Un mot de passe doit, pour être efficace, comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

III.3 Périphériques USB

Les utilisateurs ne peuvent pas connecter de périphériques USB personnels sans l'autorisation préalable du secrétaire général et du service informatique. Les périphériques doivent être donnés à la DSI pour scan de programmes potentiellement malveillants, les fichiers à mettre sur les périphériques sont uniquement récupérables sur les postes de la DSI.

III.4 Antivirus

La sécurité des espaces de stockage : utilisation d'antivirus.

Les ressources informatiques doivent être contrôlées par des antivirus. Des processus automatiques analysent les ressources informatiques, y compris les espaces personnels, pour détecter la présence de programmes malveillants, notamment la présence de virus informatiques, susceptibles de compromettre la sécurité de ces ressources ou celle de ressources externes à l'équipement.

Le rôle de ces processus automatiques est de permettre aux administrateurs de mettre ces programmes malveillants hors d'état de nuire. Les utilisateurs sont informés que, par l'intermédiaire de l'antivirus, l'administrateur du système informatique peut avoir accès au nom des répertoires et des fichiers contenus dans les disques durs.

IV ARTICLE 3 : PAREFEU ET GESTION DE STRATEGIE DE GROUPE (GPO – Group Policy Object)

Un pare-feu FORTIGATE 60F est mis en place en amont de la structure SI. Le pare-feu vérifie tout le trafic entrant et sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique, les services VPN, les échanges de fichiers distants, les fonctionnalités Output (Messenger et échanges de fichiers) et même la navigation internet.

Il détient toutes les traces de l'activité qui transite :

- De la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- Des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe (et éventuellement texte du message).

IV.1 Dispositifs de filtrage de sites Web.

Un dispositif de filtrage de sites Web sera mis en place dans le pare-feu afin de ne pas autoriser l'accès, notamment les sites comportant des éléments à caractère violent, offensant, diffamatoire, injurieux, raciste, antisémite, xénophobe, pornographique, pédophile ou susceptible de porter atteinte au respect et à la dignité de la personne humaine.Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visées sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes. Liste des sites bloquées en annexes. Le déblocage de certains sites web à usages professionnels doit être effectué sur demande à la DSI et du secrétaire général.

IV.2 Dispositifs de filtrage de certaines applications.

La politique de l'entreprise peut interdire l'usage de certaine applications (ou logiciels) par la mise en place de filtres et de stratégie de groupe dans l'active directory. Les dispositifs et les règles de filtrage seront établis par la DSI en fonction de ses propres besoins et de ceux exprimés par les utilisateurs et en tenant compte notamment des avis du secrétaire général.

V ARTICLE 4 : UTILISATION DES RESSOURCES

V.1 Usage professionnel

L'utilisateur s'engage à n'utiliser les ressources informatiques que le groupe NP AKADIN met à sa disposition qu'à seule fin professionnelle. Les activités professionnelles sont les activités de recherche de développement technique, veille technologique, d'établissement de planning de travail, plans d'exécutions, rapports et suivi, rédaction d'email ainsi que toute activité administrative, de gestion découlant ou accompagnant ces activités. Toutefois, une utilisation personnelle est autorisée dans les cas d'urgence et de nécessité. En outre, elle est tolérée sous réserve de ne pas nuire au temps consacré au travail ni à la qualité de celui-ci, de ne pas entraver le bon fonctionnement du service ni des ressources informatiques et en respectant la législation civile et pénale en vigueur. L'outil et les ressources informatiques ne peuvent être utilisés à des fins de propagande politique ou religieuse.

Toute information ou donnée, tout fichier, répertoire ou dossier, ainsi que tout message est considéré comme professionnel s'il n'est pas expressément « identifié » comme personnel ou privé.

V.2 Poste de travail

L'utilisation des ressources informatiques du groupe NP AKADIN, notamment l'ouverture d'un compte ou la connexion d'un équipement sur le réseau du groupe est soumise à autorisation avec compte utilisateur.

Ces autorisations et comptes utilisateurs sont strictement personnels et ne peuvent en aucun cas être cédés, même temporairement, à un tiers. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée, sauf cas particulier, ainsi qu'en cas de manquements graves ou répétés à la présente charte. L'utilisation d'équipements informatiques mobiles raccordés au réseau doit faire l'objet d'une validation préalable par la DSI, qui vérifie la conformité de l'équipement aux réseaux du groupe ainsi que sa protection contre les virus et les intrusions.

Lorsqu'il quitte un poste de travail, il doit verrouiller ou fermer les sessions ouvertes afin de ne pas laisser des ressources ou des services disponibles sans identification.

V.3 Contrôle d'accès et pointage

Chaque collaborateur sera enregistré dans les contrôleurs d'accès de l'entreprise et obtiendra les droits respectifs pour les zones qui leur sont accessible. Le contrôle des accès se fera par reconnaissance faciale. Toute personne extérieure au groupe NP AKADIN pourra accéder aux locaux uniquement par l'utilisation d'un badge visiteur donné par le service d'accueil principal.

Chaque collaborateur doit effectuer leur pointage d'entrée et de sortie à leur poste en utilisant la reconnaissance par empreinte digitale, ces informations seront enregistrées automatiquement dans la base de données RH pour contrôle des heures de travail et la ponctualité du collaborateur.

V.4 Utilisation des MFP

L'accès au MFP se fera par un mot de passe, toute activité sur le MFP sera enregistrée dans le journal des travaux du MFP.

Les MFP sont uniquement à usage professionnels, chaque impression sera envoyée en impression privée protégé par mot de passe afin d'éviter le vol d'information confidentielle ;

Les impressions envoyées restent pendant 30 minutes dans la file d'attente du MFP, si le collaborateur ne valide pas l'impression pendant ce temps imparti, l'élément en attente sera automatiquement supprimé, ceci dans le but d'éviter le gaspillage de papier ;

Les scans seront envoyés automatiquement sur le serveur de fichiers partagés et peuvent être récupérés sur les postes de travails à travers le réseau ;

V.5 Les interdictions à respecter par tout utilisateur

Il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.

Il ne doit pas tenter de lire, modifier, déposer ou détruire des données sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.

Il ne doit pas tenter de lire, modifier, déposer ou détruire des données détenues par d'autres utilisateurs, même si ces données ne sont pas explicitement protégées, sauf autorisation expresse des intéressés.

Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.

Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.

Il ne doit pas connecter un matériel sur le réseau sans autorisation préalable de la DSI et du secrétaire général. Cette interdiction concerne, en priorité, les visiteurs et les partenaires.

Il ne doit pas mettre à la disposition de personnes non autorisées un accès aux ressources informatiques.

Il ne doit pas, par quelque moyen que ce soit, proposer ou rendre accessible aux tiers des informations confidentielles.

Il ne doit pas télécharger ou diffuser des données en violation des lois protégeant les droits d'auteur, quel que soit le domaine (écrits, images, logiciels, bases de données…).

Il ne doit pas contourner les restrictions d'utilisation d'un logiciel.

Il ne doit pas utiliser les listes de diffusion institutionnelles hors du cadre strictement professionnel, sauf autorisation du secrétaire général.

V.6 Responsabilité générale

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques mises à sa disposition et s'engage à ne pas effectuer volontairement des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement de ces ressources, sur l'intégrité des systèmes d'information et sur les relations internes et externes du groupe NP AKADIN.

Chaque utilisateur a la charge, à son niveau, de contribuer à la sécurité générale des systèmes d'information. Il s'interdit notamment toute manipulation anormale et tout introduction de ressources non autorisées et s'engage à respecter les procédures de sécurité communiquées par la DSI et, particulièrement, les procédures d'authentification. L'utilisation des ressources informatiques doit être rationnelle et conforme à l'intérêt du service, contribuant ainsi à éviter sa saturation ou son détournement. Toute anomalie constatée, susceptible d'affecter la sécurité des ressources informatiques, doit être signalée à l'équipe informatique. Le GROUPE NP AKADIN ne pourra être tenu pour responsable des détériorations d'informations ou des manquements commis par un utilisateur qui ne se sera pas conformé à ces règles. Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur.

VI GUIDE D'UTILISATION DES RESSOURCES

La DSI se chargera au fur et à mesure de communiquer des manuels, documents et organisera des formations sur l'utilisation de chaque ressource informatique.

Les documents seront communiqués aux responsables de chaque pôle par voie électronique ou papier.

Chaque collaborateur est libre de contacter la DSI pour toutes questions ou demande d'assistance sur l'utilisation des ressources informatiques, la DSI reste entièrement disponible et se trouve au service de tout collaborateur au sein du groupe NP AKADIN.

La charte sur validation du secrétaire général est appliquée et demeure en vigueur jusqu'à publication d'une mise à jour ou sur nouvel ordre. Elle reste un outil essentiel pour une utilisation responsable et sécurisée des ressources informatiques de l'entreprise.

Afin de tenir compte du contexte juridique et technologique en rapide évolution en matière de technologies de l'information, la charte sera réactualisée régulièrement et les utilisateurs en seront informés. La DSI organisera également des formations adaptées pour fournir des informations complémentaires sur l'application de la charte.

Tout collaborateur se doit dans l'obligation de lire et signer avec la mention « Lu et approuvé » la présente charte afin d'accéder pleinement aux ressources informatiques.

Collaborateur	DSI / RSI	SECRETAIRE GENERAL