NET BY US Sarl

SOCIETE DE SERVICES NUMERIQUES

N°IFU : 3201702215012

Adresse : Ilot : 1191, Cadjehoun, Cotonou, Maison Gatien HOUNGBEDJI

Numéro de téléphone : 01 69 79 12 12

MODELE DE CHARTE INFORMATIQUE

NET BY US Sarl met à disposition des utilisateurs du matériel informatique, un Système d'Information (SI) et des moyens informatiques nécessaires à l'exécution de ses missions et de ses activités.

Celui-ci comprend :

- Un réseau informatique
- Un réseau téléphonique
- Des ordinateurs portables
- Des écrans
- Périphériques d'entrée (Clavier et souris)
- Les Logiciels Essentiels
- Les Outils et plateformes de développement

Dans le cadre de leurs fonctions, les utilisateurs sont conduits à utiliser les ressources informatiques mises à leur disposition par l'entreprise.

Dans un objectif de transparence, la présente Charte définit les règles dans lesquelles ces ressources peuvent être utilisées.

Article 1 : Utilisateurs concernés

La présente Charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

- Les dirigeants
- Les salariés
- Les intérimaires
- Les stagiaires
- Les employés de sociétés prestataires
- Les visiteurs occasionnels

Il appartient aux salariés de **NET BY US Sarl** de s'assurer de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au Système d'Information.

Article 2 : Caractéristiques du Système d'Information

Le système d'information est composé (Préciser les composantes) des ressources suivantes :

- Ordinateurs
- Téléphones
- Réseau informatique (serveurs, routeurs et connectiques)
- Photocopieurs
- Logiciels
- Données informatisées
- Messagerie

Aux fins d'assurer la sécurité informatique du Système d'Information, tout matériel connecté au SI de l'entreprise, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente Charte.

Article 3 : Règles générales d'utilisation

Le Système d'Information doit être utilisé à des fins professionnelles, conformes aux objectifs de l'organisation, sauf exception prévue par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser le Système d'Information de **NET BY US Sarl** pour se livrer à des activités concurrentes et/ou susceptibles de porter préjudice à l'organisation de quelque manière que ce soit.

Article 4 :

NET BY US Sarl met en œuvre une série de moyens pour assurer la sécurité de son Système d'Information et des données traités, en particulier des données personnelles. A ce titre elle peut limiter l'accès à certaines ressources.

4.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiés dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence.

Chaque utilisateur s'engage à :

- Utiliser les outils informatiques exclusivement à des fins professionnelles, sauf tolérance spécifique accordée par la DSI.
- Protéger ses identifiants et mots de passe. Ceux-ci sont strictement personnels et ne doivent être ni partagés ni communiqués.
- Verrouiller sa session lorsqu'il quitte son poste.
- Respecter la confidentialité des données auxquelles il a accès.
- Signaler immédiatement la DSI de toute anomalie, suspicion de piratage ou perte d'équipement.

4.2 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le système d'information de l'organisation.

Régime de Propriété et de Confidentialité :

- Propriété exclusive : Toutes les données stockées, traitées ou transmises via le Système d'Information (SI) de NETBYUS sont la propriété exclusive de l'entreprise et/ou des clients pour le compte desquels elles sont manipulées. L'utilisateur n'acquiert aucun droit de propriété sur ces données.
- Obligation de confidentialité renforcée : L'accès aux données clients est strictement limité aux besoins du projet. Cette obligation de confidentialité est absolue et perdure après la fin de la mission ou du contrat de travail.

4.3 Mot de Passe

L'accès aux Système d'Information ou aux ressources informatiques mises à disposition doit être protégé par un mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun.

Exigences en matière de mots de passe

Les mots de passe doivent impérativement respecter les critères de robustesse et de gestion suivants :

- Longueur et complexité **:** Le mot de passe doit contenir un minimum de **12 caractères** et être complexe, incluant une combinaison de lettres minuscules, de majuscules, de chiffres et de symboles.
- Périodicité **:** Le renouvellement du mot de passe est rendu **obligatoire tous les 90 jours** par le système de gestion des identités.
- Confidentialité absolue : Le mot de passe ne doit jamais être communiqué à un tiers, y compris à un membre de la DSI. Il est interdit de le noter en clair sur un support papier ou électronique non chiffré.

Authentification Multi-Facteurs (MFA)

- MFA obligatoire **:** L'usage de l'authentification multi-facteurs (MFA) est obligatoire pour tous les accès jugés sensibles ou critiques par la DSI.
- Périmètre **:** Le MFA est notamment requis pour l'accès aux boîtes e-mails professionnelles, aux environnements de production et aux plateformes de gestion des clients. L'utilisateur doit se conformer au dispositif (clé physique) fourni par l'entreprise.

4.4 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

La sécurité physique du matériel est une responsabilité de l'utilisateur et un prérequis à la confidentialité.

- Verrouillage Systématique : La session de travail doit être systématiquement verrouillée (Clean Screen) dès que le poste est laissé sans surveillance, même pour une très courte absence.
- Gestion des Absences : En cas d'absence prolongée (réunion externe, fin de journée), le matériel doit être éteint ou mis en veille sécurisée et rangé conformément à la politique Clean Desk.

4.5 Installation de logiciels

L’utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l’accord du service informatique en raison notamment du risque de virus informatiques.

Configuration technique et installation logicielle

Le maintien d'une configuration logicielle et système uniforme est un prérequis à la sécurité et à la maintenance du Système d'Information.

- Logiciels approuvés uniquement : L'utilisateur est strictement interdit d'installer, de désinstaller, de mettre à jour ou de modifier tout logiciel, extension de navigateur, ou application mobile sans l'approbation préalable et documentée de la DSI.
- Configurations système : Il est interdit de modifier les configurations système critiques de l'équipement, notamment :

1) La désactivation des mécanismes de sécurité (antivirus, pare-feu, chiffrement du disque).
2) La modification des paramètres réseau ou de l'accès VPN.
3) La création de comptes d'utilisateur locaux non autorisés.

- Mises à Jour : L'utilisateur est tenu de se conformer aux fenêtres de maintenance et d'appliquer dans les délais les mises à jour et correctifs de sécurité déployés à distance par la DSI.

4.6 Copie de données informatiques

La gestion de la conservation et la sauvegarde des données garantit la résilience de notre activité et le respect des obligations légales d'archivage et de destruction.

Centralisation et responsabilité des sauvegardes

- Responsabilité DSI : La Direction des Systèmes d'Information (DSI) est l'unique entité responsable de la mise en œuvre, de la gestion, de la vérification et de la maintenance des systèmes de sauvegarde de l'ensemble du Système d'Information (serveurs, bases de données, environnements Cloud critiques).
- Vérification de la Restauration : La DSI s'engage à tester périodiquement l'intégrité et la capacité de restauration des sauvegardes, conformément au Plan de Reprise d'Activité (PRA) de l’entreprise.
- Durée de Conservation : La durée de conservation des données et des archives est définie par la DSI en collaboration avec le service juridique, en respectant les impératifs légaux et les exigences contractuelles des clients.

Interdiction des copies et sauvegardes locales

- Principe d'Interdiction : Les collaborateurs ne doivent en aucun cas créer des copies locales, des archives personnelles ou des sauvegardes non sécurisées des données de l'entreprise ou des clients sur leurs postes de travail, disques durs externes ou supports non gérés par la DSI.
- Risque : Ces copies locales non sécurisées représentent un risque majeur en cas de vol, de défaillance matérielle (non couvert par la sauvegarde centralisée) ou d'attaque par rançongiciel, exposant l'entreprise et ses clients à une perte ou une fuite de données.

- Stockage Unique : Les données de travail (documents, code source) doivent être stockées exclusivement sur les emplacements réseau (serveurs de fichiers, plateformes collaboratives) fournis par l'entreprise, seuls lieux soumis à la politique de sauvegarde centralisée et sécurisée.
- Effacement : L'utilisateur a l'obligation de s'assurer que les données temporaires ou les copies de travail sont effacées de son poste local dès que leur traitement est terminé et qu'elles ont été enregistrées sur le stockage sécurisé et centralisé.

Article 5 : Modalités d'utilisation des ressources informatiques

Le matériel informatique mis à disposition de l'utilisateur est un outil de travail dont l'intégrité est indispensable à la continuité de notre service.

- Propriété de l'entreprise **:** L'ensemble du matériel (ordinateurs portables, postes de travail fixes, écrans, périphériques, téléphones mobiles, cartes SIM, etc.) est et demeure la **propriété exclusive de NETBYUS**. Ce matériel est inventorié et traçable.
- Devoir de soin et de préservation **:** L'utilisateur a l'obligation d'en prendre soin et de l'utiliser conformément aux instructions du fabricant et de la DSI. Il doit le protéger contre les chocs, les liquides, la chaleur excessive et toute altération non autorisée.
- Rapports de dommages **:** Tout dommage, panne ou dysfonctionnement doit être signalé immédiatement à la DSI. L'utilisateur pourra être tenu responsable des dommages causés au matériel par négligence ou mauvaise utilisation.

Article 6 : Accès à internet

L'accès à Internet et aux réseaux externes est un privilège accordé dans le but exclusif de faciliter l'activité professionnelle de l'utilisateur.

Finalité professionnelle

- Priorité absolue **:** L'accès Internet mis à disposition par **NETBYUS** est un outil destiné en priorité à la recherche d'informations, à l'utilisation d'applications métiers et à la communication nécessaires à l'exécution des missions.
- Usage personnel toléré **:** L'usage à des fins personnelles est toléré sous réserve qu'il soit raisonnable en volume et en fréquence, qu'il soit effectué en dehors du temps de travail effectif ou pendant les pauses, et qu'il ne porte en aucun cas atteinte à la sécurité du SI ou à la réputation de l'entreprise.

Restrictions de contenu et éthique

- La consultation, le partage ou le téléchargement de contenus enfreignant la loi ou nuisant à l'image de l'entreprise est strictement et formellement interdit. Ceci inclut, sans s'y limiter :
- Les sites à caractère illégal, haineux, raciste, discriminatoire ou faisant l'apologie du terrorisme.
- La consultation de sites à caractère pornographique ou violent.
- L'accès et la participation excessive à des forums, réseaux sociaux ou plateformes à des fins politiques, religieuses ou personnelles portant atteinte à l'environnement de travail.

- La diffusion d'informations confidentielles ou l'usurpation d'identité.

Interdiction de téléchargement et de logiciels non autorisés

- Téléchargement illégal **:** Le téléchargement, le partage, la diffusion ou l'utilisation de contenus protégés par le droit d'auteur (logiciels, musique, films, vidéos) sans licence valide est strictement prohibé. Ces activités engagent la responsabilité pénale et civile de l'entreprise.
- Logiciels et jeux **:** L'installation de logiciels personnels ou de jeux vidéo sur les équipements de l'entreprise est interdite.
- Consommation de bande passante **:** L'utilisateur doit s'abstenir de toute activité en ligne consommant inutilement une bande passante significative, de manière à ne pas dégrader la qualité du service pour les autres collaborateurs ou les applications critiques (ex. : streaming vidéo excessif).

Mesures de contrôle et de filtrage

- Filtrage **:** La DSI met en place des outils de filtrage et de proxy pour bloquer l'accès aux sites identifiés comme dangereux, illégaux ou incompatibles avec les valeurs et la sécurité de l'entreprise.
- Journalisation (*Logs***) :** L'entreprise se réserve le droit de journaliser les connexions Internet des utilisateurs (conservation des adresses IP et des domaines consultés) à des fins de maintenance, de sécurité, de défense en cas de contentieux, et pour s'assurer du respect de cette charte. Cette journalisation est effectuée dans le respect des règles légales et des recommandations de l'APDP.

Article 7 : TÉLÉTRAVAIL, MOBILITÉ ET ACCÈS SÉCURISÉ À DISTANCE

L'utilisateur en situation de télétravail ou de mobilité a l'obligation de recréer un environnement sécurisé équivalent aux locaux de l'entreprise.

Environnement de télétravail et exigences sécurité

- Sécurité domiciliaire **:** Le lieu de télétravail (domicile ou autre lieu autorisé) doit garantir un niveau de sécurité physique et logique suffisant. L'utilisateur est responsable de la sécurisation physique des équipements.

- Confidentialité de l'espace **:** L'utilisateur doit s'assurer que son espace de travail préserve la stricte confidentialité des informations traitées. Les documents sensibles (physiques ou à l'écran) doivent être à l'abri des regards de tiers non autorisés (famille, colocataires, visiteurs).

- Réseau domestique **:** La connexion internet domestique utilisée pour le télétravail doit être sécurisée (mot de passe Wi-Fi fort, protocole WPA2 ou WPA3). L'utilisation de réseaux Wi-Fi publics ou ouverts pour le traitement de données confidentielles est formellement interdite.

- Isolation des équipements **:** Il est interdit de connecter des appareils personnels non gérés (consoles de jeux, téléviseurs connectés) au même réseau que le matériel professionnel lorsque celui-ci est utilisé pour des tâches sensibles.

Exigences de connexion et d'authentification à distance

L'accès aux ressources internes et clients est strictement conditionné à l'application de mesures de sécurité renforcées.

- VPN d'entreprise obligatoire **:** Toutes les connexions vers le Système d'Information de **NETBYUS**, vers les serveurs de fichiers, les applications critiques, ou les environnements de production clients, doivent impérativement transiter par le Réseau privé virtuel (VPN) fourni et géré par la DSI.

  1) Le VPN assure le chiffrement du flux de données et maintient l'intégrité de la communication.

- Authentification Multi-Facteurs (MFA**) :** L'accès au VPN, ainsi qu'aux boîtes e-mails et aux plateformes de gestion des projets (Cloud, DevOps), requiert l'utilisation systématique de l'Authentification Multi-Facteurs (MFA).

Gestion du matériel et des données en mobilité

- Stockage exclusif **:** Les documents professionnels, les codes sources, les bases de données et toute information client ne doivent en aucun cas être stockés, même temporairement, sur des appareils personnels (ordinateurs, smartphones, tablettes) ou des solutions de stockage Cloud personnelles (Dropbox, Google Drive, etc.).

- Appareils autorisés **:** Seuls les équipements fournis, configurés et inventoriés par l'entreprise sont autorisés pour l'accès aux environnements sensibles.

- Transport du matériel **:** Le matériel portable (ordinateur, smartphone) doit être transporté avec le plus grand soin. L'utilisateur est responsable de signaler immédiatement tout dommage, perte ou vol.

- Accès aux outils d'administration **:** L'accès aux outils de production, aux consoles d'administration (*root*), et aux systèmes d'information critiques est réservé à une liste d'utilisateurs nominativement autorisés. Ces accès sont journalisés, supervisés et requièrent des mesures d'authentification encore plus strictes.

Article 8 : Email

La gestion de l'identité numérique est la fondation de notre sécurité.

- Identifiant unique : Chaque utilisateur se voit attribuer un identifiant personnel et unique pour l'accès au Système d'Information (SI). Cet identifiant est strictement personnel et ne doit jamais être cédé, prêté, ou partagé.
- Interdiction d'usurpation : L'usurpation d'identité, l'utilisation du compte d'un tiers ou l'utilisation d'un compte générique non nominatif (sauf compte de service technique formellement identifié) est formellement interdite.

Article 9 : Sanctions

Les manquements aux règles édictées par la présente Charte peuvent engager la responsabilité de l'utilisateur et entrainer des sanctions internes propres à **NET BY US Sarl** à son encontre et celles prévues par les dispositions des articles 425 et 426 du Livre V^{ème} du code du numérique. Il s'agit des :

Sanctions disciplinaires

Tout manquement aux dispositions de la présente charte sera considéré comme une faute professionnelle engageant la responsabilité de l'utilisateur. L'entreprise appliquera l'échelle des sanctions disciplinaires prévue par le Règlement Intérieur, pouvant aller de l'avertissement au licenciement pour faute grave, selon la gravité de l'infraction, l'existence d'une intention de nuire et l'éventuel préjudice causé.

Poursuites judiciaires

En cas de violation grave entraînant un préjudice matériel ou de réputation (vol de données, fraude informatique, violation de données à caractère personnel, téléchargement illégal), l'entreprise se réserve le droit d'engager des poursuites judiciaires (civiles ou pénales) contre l'auteur du manquement.

Article 10 : Règles et procédures en cas de départ définitif

La procédure de départ (fin de contrat, démission, licenciement) est encadrée par des règles strictes de sécurité.

- Obligation de restitution : En cas de départ de l'entreprise (quelle qu'en soit la raison), l'utilisateur a l'obligation de restituer immédiatement l'intégralité du matériel mis à sa disposition (ordinateur, téléphone, clés d'accès, etc.), dans l'état où il se trouvait lors de sa remise, hormis l'usure normale.
- Restitution des données : L'utilisateur doit s'assurer que toutes les données professionnelles (fichiers clients, code source, e-mails) sont stockées sur les serveurs de l'entreprise et accessibles à son manager ou à son successeur. Il est interdit de conserver ou de supprimer des données professionnelles ou clients au moment de son départ.
- Transfert : La DSI procédera à la désactivation des comptes et, si nécessaire, au transfert des données de l'utilisateur avant la restitution physique du matériel.

Article 1 : Information et entrée en vigueur

La présente Charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque employé.

Elle entre en vigueur en Novembre 2025. Elle est révisée périodiquement (au moins tous les deux ans) par la DSI pour s'adapter aux évolutions technologiques et réglementaires.

Fait le 01 décembre 2025

HOUNTON Ricardo