CHARTE INFORMATIQUE DU GROUPE GODET

Version	1.0
Date entrée en vigueur	29/10/2026
Rédacteur	Soumaya DRIDI - System & Data manager
Approbateur	Alex LAMBERIO - CEO

1. Préambule et champ d'application

La présente charte informatique (ci-après « la Charte ») définit les règles d'utilisation des systèmes d'information, équipements numériques et ressources réseau mis à disposition des salariés par GROUPE GODET (ci-après « l'Entreprise »).

La présente charte s'applique :

- aux salariés du Groupe Godet, dans le cadre du pouvoir de direction et du règlement intérieur ;
- aux intérimaires et salariés de prestataires intervenant sur les sites du Groupe Godet, dans le cadre des obligations de sécurité et de confidentialité résultant des contrats conclus avec leurs employeurs respectifs.

Les manquements à la présente charte commis par des intérimaires ou des salariés de prestataires sont signalés à leur employeur, qui demeure seul compétent pour décider des sanctions disciplinaires à leur égard. Le Groupe Godet se réserve la possibilité de mettre fin à la mission ou au contrat de prestation dans les conditions prévues par lesdits contrats.

La Charte est établie conformément à la législation française en vigueur, notamment :

- La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés) ;
- Le Règlement (UE) 2016/679 du 27 avril 2016 dit RGPD ;
- Le Code du travail (articles L.1121-1, L.1222-4 et suivants) ;
- La jurisprudence de la Cour de cassation et les délibérations de la CNIL.

La présente charte informatique constitue une annexe au règlement intérieur du Groupe Godet. Elle a été soumise pour information et consultation au Comité Social et Économique (CSE) en date du 07/07/2026 et communiquée à l'inspection du travail, conformément aux articles L.1321 et R1321-4 du Code du travail. Elle est opposable à l'ensemble des salariés du Groupe Godet dans les mêmes conditions que le règlement intérieur.

2. Ressources informatiques concernées

2.1 Matériels

- Ordinateurs fixes et portables ;
- Terminaux de production ;
- Téléphones fixes et mobiles professionnels ;
- Tablettes et équipements nomades ;
- Imprimantes, scanners et copieurs multifonctions ;
- Équipements de stockage (clés USB, disques durs fournis par l'Entreprise) ;
- Équipements réseau : bornes Wi-Fi, routeurs, commutateurs.

2.2 Logiciels et services

- Système d'information (ERP, PIM, GPAO) ;
- Suite bureautique et messagerie professionnelle ;
- Dossiers communs, intranet et outils de collaboration internes ;
- Accès Internet et VPN d'accès à distance ;
- Tout logiciel installé ou accessible via les équipements de l'Entreprise.

2.3 Réseaux

- Réseau local (LAN) de chaque site ;
- Liaisons inter-sites (WAN) ;
- Accès Internet fourni par l'Entreprise.

3. Règles générales d'utilisation

3.1 Usage professionnel

Les ressources informatiques sont mises à disposition des salariés pour l'exercice de leurs fonctions professionnelles. Conformément à la jurisprudence de la Cour de cassation, un usage personnel raisonnable et occasionnel est toléré, dans la mesure où cet usage :

- N'entrave pas l'activité professionnelle de l'utilisateur ni de ses collègues ;
- Ne génère pas de charge excessive sur le réseau ou les systèmes ;
- Ne nuit pas à l'image ou aux intérêts de l'Entreprise ;
- Respecte les dispositions légales et réglementaires.

Il est formellement interdit d'utiliser les ressources informatiques pour :

- Exercer une activité professionnelle personnelle ou commerciale extérieure ;
- Accéder, télécharger ou diffuser des contenus illicites, pornographiques, violents, discriminatoires ou portant atteinte à la dignité humaine ;
- Se livrer à des actes de harcèlement, d'intimidation ou de dénigrement ;
- Participer à des activités de jeux en ligne à caractère commercial.

3.2 Identifiants et mots de passe

Chaque utilisateur dispose d'identifiants nominatifs et personnels. Il est responsable de toutes les actions effectuées sous ses identifiants.

- Les mots de passe doivent comporter au minimum 12 caractères, mêlant majuscules, minuscules, chiffres et caractères spéciaux ;
- Ils doivent être changés au moins tous les 90 jours, ou immédiatement en cas de suspicion de compromission ;
- Il est interdit de communiquer ses identifiants à un tiers, quel qu'il soit ;
- L'utilisation d'un gestionnaire de mots de passe agréé par le service informatique est recommandée.

3.3 Poste de travail et messagerie

- L'utilisateur doit verrouiller sa session dès qu'il quitte son poste, même brièvement (raccourci Windows + L ou équivalent) ;
- Les fichiers à caractère personnel doivent être stockés dans un dossier clairement identifié comme tel, distinct des dossiers professionnels ;
- Les pièces jointes d'origine inconnue ou suspecte ne doivent pas être ouvertes sans vérification préalable auprès du service informatique ;
- L'utilisation d'un compte de messagerie personnel (Gmail, Outlook.com, etc.) pour traiter des affaires professionnelles est interdite.

3.4 Bon usage et entretien du matériel

Chaque utilisateur est responsable du bon état du matériel qui lui est confié. Il s'engage à :

- Manipuler les équipements avec soin et à les protéger contre tout risque de détérioration (chocs, liquides, chaleur excessive, etc.) ;
- Signaler sans délai toute panne, dégradation ou anomalie au service informatique, sans tenter de réparer soi-même l'équipement ;
- Ne pas déplacer, modifier ou démanteler un équipement sans autorisation préalable ;
- Ranger et sécuriser les équipements nomades (ordinateurs portables, tablettes, téléphones) lorsqu'ils ne sont pas utilisés, en particulier lors de déplacements professionnels ;
- Restituer le matériel en bon état de fonctionnement à la fin du contrat de travail ou sur demande de la Direction.

En cas de dommage causé aux biens, matériels ou équipements mis à sa disposition par l’employeur, la responsabilité civile et pécuniaire du salarié à l’égard de l’employeur pourra être engagée en cas de faute lourde.

4. Accès à Internet et aux réseaux

4.1 Navigation Internet

L'accès à Internet est fourni dans un cadre professionnel. Les catégories de sites suivantes sont bloquées par filtrage technique :

- Sites de téléchargement illégal (piratage, warez) ;
- Sites à contenu pornographique ou violent ;
- Sites de jeux d'argent ;
- Logiciels de contournement (proxy anonymisants, tunnels VPN non agréés) ;
- Plateformes de partage de fichiers peer-to-peer.

Un usage raisonnable des réseaux sociaux à titre personnel est toléré pendant les temps de pause. Tout usage professionnel des réseaux sociaux doit respecter les règles de communication définies par la Direction.

4.2 Télétravail et accès distant

- L'accès à distance aux systèmes de l'Entreprise est exclusivement autorisé via le VPN fourni par le service informatique ;
- L'utilisation de réseaux Wi-Fi publics non sécurisés pour accéder aux ressources internes est interdite sans VPN actif ;
- L'utilisateur en télétravail est responsable de la confidentialité de son environnement de travail.

Plus généralement, le salarié s'engage à utiliser les équipements fournis par l'entreprise.

4.3 Spécificités des sites de production

- Les équipements des lignes de production (automates, SCADA, IHM) sont sur des réseaux séparés (OT/IT segmentation) et ne doivent en aucun cas être connectés au réseau bureautique sans autorisation expresse du responsable informatique ;
- L'introduction de tout équipement externe (ordinateur portable personnel, clé USB, disque dur) sur le réseau de production est strictement interdite ;
- Toute intervention sur les équipements informatiques industriels est soumise à validation préalable du service informatique et du responsable de production.

5. Sécurité des systèmes d'information

5.1 Obligations de l'utilisateur

1. Signaler immédiatement tout incident de sécurité (virus, phishing, comportement anormal d'un équipement, perte ou vol d'un matériel) au service informatique via un email à data@godet.fr ;
2. Ne jamais désactiver ou contourner les dispositifs de sécurité (antivirus, pare-feu, filtres web) ;

3. Ne pas installer de logiciels non approuvés par le service informatique sur les équipements de l'Entreprise ;
4. Ne pas connecter de supports amovibles personnels (clés USB, disques durs, téléphones) sans autorisation préalable.

5.2 Gestion des données et confidentialité

Les données traitées dans le cadre de l'activité professionnelle sont confidentielles. Les utilisateurs s'engagent à :

- Ne pas divulguer d'informations confidentielles (données clients, procédés industriels, données financières) à des tiers non autorisés ;
- Stocker les données sensibles exclusivement sur les serveurs ou espaces de stockage agréés par l'Entreprise (et non sur des services de cloud public non approuvés) ;
- Appliquer les niveaux de classification des données définis par la politique de sécurité de l'Entreprise.

Les données, fichiers, documents, bases de données et informations créés, reçus, traités ou stockés par le salarié dans le cadre de l'exercice de ses fonctions, quel que soit leur support (ordinateur, serveur, messagerie, outils collaboratifs, cloud professionnel, etc.), sont la propriété exclusive de l'entreprise. Le salarié s'engage à ne pas supprimer, altérer, exporter, transférer ou s'approprier ces données sans autorisation préalable de sa hiérarchie, y compris en cas de départ de l'entreprise, quel qu'en soit le motif.

5.3 Mises à jour et maintenance

- Les mises à jour de sécurité sont déployées automatiquement par le service informatique ; les utilisateurs doivent les réaliser dans un bref délai ;
- En cas de maintenance planifiée, les utilisateurs s'engagent à sauvegarder leurs travaux en cours et à coopérer avec le service informatique.

6. Protection des données personnelles (RGPD)

Conformément au RGPD et à la loi Informatique et Libertés, l'Entreprise informe les salariés que des données à caractère personnel les concernant sont collectées dans le cadre de la gestion des accès informatiques et du contrôle de l'utilisation des ressources. Ces traitements sont fondés sur l'intérêt légitime de l'Entreprise (sécurité du SI) et sur le respect d'obligations légales.

L'utilisation des données est strictement proportionnée au but poursuivi. A titre d'exemple :

- sécurité des systèmes d'information ; prévention et détection des incidents de sécurité, des intrusions, des virus ou des comportements anormaux susceptibles de compromettre l'intégrité, la disponibilité ou la confidentialité des données ;
- maintenance et audit technique des systèmes ;
- À titre exceptionnel, et en cas de nécessité avérée, les logs peuvent être utilisés pour vérifier le respect par un salarié de ses obligations professionnelles, lorsque :

- un incident grave est constaté ou suspecté fraude, fuite de données, atteinte à la sécurité ;
- les autres moyens de vérification se révèlent insuffisants ;

Dans ce cas, l'utilisation des logs à des fins de contrôle individuel est réalisée dans le respect du Code du travail, du règlement général sur la protection des données RGPD et après information du salarié concerné, sauf si cette information compromet la finalité du contrôle.

6.1 Données collectées

- Identifiants de connexion et logs d'accès ;
- Adresses IP et données de navigation (URLs visitées, volumétrie) ;
- Données de messagerie (expéditeur, destinataire, objet, volumétrie – pas le contenu) ;
- Alertes générées par les outils de cybersécurité.

6.2 Droits des salariés

Conformément aux articles 15 à 22 du RGPD, les salariés disposent des droits suivants sur leurs données personnelles :

- Droit d'accès, de rectification et d'effacement (dans les limites légales) ;
- Droit à la limitation du traitement et droit d'opposition ;
- Droit à la portabilité des données.

Ces droits s'exercent auprès du Délégué à la Protection des Données (DPO) ou, à défaut, de la Direction, à l'adresse suivante : **lsantos@godet.fr**

6 bis. Utilisation des outils d'intelligence artificielle (IA)

L'essor des outils d'intelligence artificielle générative (ChatGPT, Copilot, Gemini, Claude, etc.) conduit l'Entreprise à encadrer leur usage dans un cadre professionnel.

Principe général L'utilisation d'outils d'IA à des fins professionnelles est autorisée sous réserve du respect des présentes règles. Elle ne dispense pas le salarié d'exercer son jugement et sa responsabilité sur les contenus produits.

Données interdites Il est strictement interdit de soumettre à un outil d'IA externe les données suivantes :

- Données personnelles de salariés, clients ou partenaires (noms, coordonnées, données RH, etc.) ;
- Informations confidentielles de l'entreprise :
  - Données financières confidentielles (résultats, budgets, contrats, offres commerciales) ;
  - Informations relatives aux procédés industriels, savoir-faire et secrets de fabrication ;
  - Tout document classifié « confidentiel » ou « usage interne » selon la politique de l'Entreprise ;

Plus largement, toutes informations non publiques de l'entreprise, notamment des secrets d'affaires, des informations financières non publiques, des données techniques.
- Identifiants, mots de passe ou toute information d'accès aux systèmes.

Rappel technique important Les outils d'IA grand public fonctionnent via des serveurs externes. Toute donnée saisie peut être utilisée pour entraîner les modèles ou être exposée à des tiers. L'Entreprise ne peut garantir la confidentialité des informations transmises à ces services.

Outils approuvés Seuls les outils d'IA expressément approuvés par le service informatique et/ou la Direction peuvent être utilisés pour traiter des données internes sensibles. La liste des outils approuvés est disponible auprès du responsable informatique.

Vérification des contenus générés Le salarié reste seul responsable des contenus produits à l'aide d'un outil d'IA et utilisés dans le cadre professionnel. Toute information générée doit être vérifiée avant diffusion ou utilisation.

Politique RSE – Adopter un usage éthique et environnemental Adopter un usage raisonné et proportionné des outils IA ; une recherche simple consomme environ 0,3 Wh (≈ 0,2 g de CO_2), contre près de 2 Wh (≈ 2 g CO_2) pour une requête générative.

7. Contrôle et surveillance des utilisateurs

L'Entreprise se réserve le droit de procéder à des contrôles des ressources informatiques mis à disposition des salariés, dans le respect du cadre juridique applicable (avis CNIL, jurisprudence de la Cour de cassation et du Conseil d'État).

7.1 Modalités du contrôle

- Les contrôles sont réalisés par le service informatique habilité, sous l'autorité de la Direction ;
- Ils portent sur les journaux de connexion, l'utilisation de la messagerie (métadonnées), la navigation Internet et les accès aux fichiers partagés ;
- L'ouverture de fichiers personnellement identifiés comme tels ne peut être réalisée qu'en présence du salarié concerné ou après qu'il a été dûment convoqué, **sauf risque ou événement particulier justifiant un accès immédiat (sécurité des systèmes, menace grave, etc.).**

7.2 Limites du contrôle

Ces contrôles :

- ne sont pas permanents, ni systématiques ;
- sont limités aux informations nécessaires à la vérification du respect des règles d'usage ;
- sont réalisés dans le respect du droit au respect de la vie privée et des correspondances et des recommandations de la CNIL.

8. Sanctions

Tout manquement aux règles définies par la présente Charte peut donner lieu, selon la gravité des faits **et le caractère répétitif**, à des sanctions disciplinaires conformément au règlement intérieur de l'Entreprise et **au Code du travail, dans le respect de la procédure disciplinaire applicable.**

La responsabilité pénale personnelle du salarié peut être engagée indépendamment de toute procédure disciplinaire, notamment en cas de fraude informatique, d'atteinte à un système de traitement automatisé de données ou de violation de données personnelles.

9. Dispositions finales

9.1 Entrée en vigueur et révision

La présente Charte entre en vigueur un mois suivant l'accomplissement des formalités de dépôt et de publicité prévues par les articles R. 1321-1 et R. 1321-2 du Code du travail. Elle sera révisée en cas d'évolution significative des technologies utilisées, de la législation applicable ou de l'organisation de l'Entreprise, et au minimum tous les deux ans.

9.2 Diffusion et acceptation

- La Charte est remise à chaque salarié lors de son embauche ou lors de sa première mise à jour, contre signature de l'attestation de prise de connaissance ci-dessous ;
- **Elle est disponible en permanence sur l'intranet de l'Entreprise ;**
- **Elle est annexée au règlement intérieur de l'Entreprise.**

9.3 Responsable informatique

Pour toute question relative à la présente Charte, les salariés peuvent contacter :

- Responsable Informatique : Soumaya DRIDI – data@godet.fr – 06 65 19 92 96
- Pour les urgences (incidents de sécurité) : Soumaya DRIDI – data@godet.fr – 06 65 19 92 96