[Nom de l’entreprise]
Charte d’usage de l’Intelligence Artificielle

Préambule

Chez [Nom de l’entreprise], nous explorons le potentiel de l’Intelligence Artificielle (IA) pour stimuler l’innovation, renforcer l’efficacité et élever la qualité de notre travail.
Notre ambition : en faire un levier d'excellence, sans jamais sacrifier la sécurité des données, l’éthique ou l’humain.
La présente charte définit les objectifs, usages autorisés, lignes directrices et engagements que chacun doit respecter.

Cette charte a valeur de politique interne obligatoire. Son non-respect expose à des sanctions disciplinaires.

Contexte et objectifs

- Inscrire l’usage de l’IA dans la stratégie de l’entreprise.
- Fixer un cadre clair pour un usage responsable, sécurisé et éthique.
- Protéger les données, la propriété intellectuelle, la réputation et l’humain.

Définitions

- **Intelligence artificielle** : systèmes capables de générer du contenu, d’analyser des données ou d'automatiser des tâches en mimant des processus cognitifs humains.
- **Utilisateurs finaux** : collaborateurs utilisant l’IA dans un cadre professionnel.
- **Déployeurs** : responsables techniques ou métiers mettant l’IA à disposition des collaborateurs.

Autres éléments à préciser :

IA générative ≠ IA analytique.

Données sensibles ≠ données confidentielles.

Utilisateurs ≠ Administrateurs ≠ Exploitants de modèles.

Responsabilité des déployeurs et des utilisateurs

- **Déployeurs** : sélectionner, valider, documenter les outils IA ; évaluer les risques et surveiller les performances.

- **Utilisateurs** : respecter les usages autorisés, vérifier systématiquement les résultats, signaler toute dérive ou anomalie.

Usages autorisés / Utilisations interdites

- **Autorisé** : gain de productivité, support à la création, analyse de données dans le respect des règles internes.

- **Interdit** : traitement non autorisé de données sensibles, génération de deepfakes, production de contenus mensongers ou contraires aux valeurs de l'entreprise.

A ajouter éventuellement : une **clause de responsabilité autonome** : l'utilisateur reste **pleinement responsable** du résultat final, même si l'usage était à la base "autorisé".

Outils d’IA approuvés

Seuls les outils listés ci-dessous peuvent être utilisés, sous réserve d'un usage conforme :

- ChatGPT

- Bing AI (Microsoft Copilot)

- Grammarly

- Descript (connexion requise)

- DALL·E (connexion requise)

- Notion

Tout autre outil doit être validé préalablement auprès du manager et du référent IA.

La liste doit être régulièrement mise à jour. Indiquer idéalement la version de l’outil concernée.

Bonnes pratiques d’usage

- Lire et comprendre la documentation des outils utilisés : fonctionnement, limites, exactitude, biais possibles.
- Exercer son esprit critique : l’IA propose, l’humain dispose.
- Vérifier systématiquement les contenus générés : recouper les informations avec des sources fiables.
- Ne jamais introduire d’informations sensibles sans anonymisation préalable.
- Respecter la propriété intellectuelle : éviter tout plagiat ou exploitation abusive d’œuvres existantes.
- Mentionner explicitement tout contenu assisté ou généré par IA.

Confidentialité, sécurité et protection des données

- Ne jamais soumettre de données personnelles sans accord explicite.
- Appliquer l'anonymisation systématique avant tout usage.
- S'assurer du niveau de sécurité de l'outil avant de l'utiliser.

Attention : "Ne jamais soumettre de données personnelles sans accord explicite" est **insuffisant** au regard du RGPD.
C'est une **analyse d'impact (DPIA)** qui est nécessaire pour tout traitement nouveau ou risqué via IA.
L’accord de la personne concernée **n’est qu’un dernier recours**.

Protection des secrets d’affaires et de la propriété intellectuelle

- Il est interdit d'utiliser un outil d'IA dont l’architecture, les sous-traitants ou les flux de données exposent un risque d’exfiltration d’informations stratégiques, même indirect.

- Il est interdit d’intégrer dans une IA tout secret industriel, donnée propriétaire ou information stratégique sensible.

- Aucun modèle d’IA ne peut être entraîné sur des données internes sans autorisation expresse.

IA, droits d’auteur et cadre légal

Le respect du droit est un pilier fondamental de notre approche.

- Propriété intellectuelle : les productions issues de l’IA peuvent contenir des éléments protégés. Il est impératif de valider les sources, garantir l’originalité des contenus et éviter toute infraction.
- Protection des données : tout usage de l’IA doit se conformer aux réglementations en vigueur (ex. : RGPD, CCPA). Aucune donnée confidentielle ne doit être transmise à une IA.

Données & Sécurité

La protection des données est non négociable. Chaque collaborateur et manager en est responsable.

- Protection des données : il est formellement interdit de partager des données réelles de clients ou des identifiants d’accès à des outils internes avec un outil d’IA.
- Contrôle d’accès : seuls les collaborateurs autorisés peuvent accéder à certaines données ou systèmes. Traitez l’IA comme un prestataire externe sans clause de confidentialité.
- Audit régulier : des audits de sécurité seront menés périodiquement afin de détecter et limiter les risques liés à l’usage de l’IA.

Formation et sensibilisation

- Formation obligatoire pour tout utilisateur d’IA.

- Modules couvrant : fonctionnement des IA utilisées, bonnes pratiques, risques liés à l’IA générative, éthique de la promptologie.

Vérification et interprétation des résultats

- Considérer toute sortie d’IA comme un **brouillon** devant être validé humainement.

- Obligation de double vérification : validation métier et comparaison avec des sources reconnues.

Lutter contre les biais de l’IA

L’IA peut reproduire ou amplifier les biais présents dans ses données d’apprentissage. Il incombe à chacun de prévenir ces dérives.

- Détection des biais : tout contenu généré par IA doit être relu, édité et corrigé pour éviter les biais sociaux ou algorithmiques.
- Données inclusives : veillez à la diversité des données d’entrée pour produire des résultats représentatifs et équitables.
- Stratégies de mitigation : formalisez et partagez avec votre manager vos approches pour corriger les biais détectés.

Respect des règles relatives aux résultats

- Interdiction de manipuler images, vidéos, sons sans avertissement explicite.

- Obligation de transparence : préciser clairement si un contenu a été assisté ou généré par IA.

Divers

Irréversibilité des données transmises à une IA externe

Tout contenu soumis à un système d'IA externe est susceptible d'être définitivement perdu pour le contrôle de l'entreprise. Même si certains fournisseurs promettent de respecter la confidentialité des données, aucune garantie technique absolue ne peut être assurée. À ce titre, toute donnée transmise peut être exploitée à des fins d’entraiînement de modèles, exposant l’entreprise à des risques majeurs de pollution informationnelle et de déperdition de ses actifs stratégiques.

Obligation d’alerte en cas de doute ou d'incident

Tout collaborateur ayant connaissance ou soupçon d'un usage non conforme de l'IA, d'une anomalie, d'une fuite de données ou d'un contenu douteux doit en informer immédiatement le référent IA et/ou le DPO.

Sanctions en cas de violation de la Charte

Toute infraction à la présente Charte expose son auteur à des mesures disciplinaires conformément aux politiques internes de [Nom de l'entreprise], pouvant aller jusqu'au licenciement pour faute grave. En cas de préjudice résultant d'un usage illicite ou négligent, des poursuites civiles ou pénales pourront être engagées.

Encadrement des tiers et prestataires

Il est strictement interdit à tout prestataire externe d'utiliser une IA sur des données de [Nom de l'entreprise] sans validation préalable écrite par le référent IA ou le DPO. Tout manquement expose le prestataire à une rupture unilatérale de contrat et à des recours juridiques.

Territorialité et transfert des données

Seules les IA respectant le périmètre de protection des données de l'Union européenne (RGPD) peuvent être utilisées. Aucun transfert de données personnelles vers des pays tiers non reconnus comme adéquats par l'UE ne sera toléré sans garanties appropriées, préalablement validées.

Absence de consentement implicite

Le recours à un outil d'IA, même de manière occasionnelle ou intuitive, n'exonère en rien l'utilisateur de ses responsabilités. L'obligation de vérification, de confidentialité et de respect des règles internes reste pleine et entière. L'automatisation ne saurait être une excuse à la défaillance.

Référent interne

- Un référent IA est désigné pour garantir le respect de la charte, répondre aux questions et gérer les incidents.

Contact :
Jane Doe
AI Officer
[email@company.com]

Mise à jour

- Révision annuelle de la charte, ou en fonction des évolutions technologiques, réglementaires ou stratégiques.
- Communication systématique de toute mise à jour aux collaborateurs concernés.

Accusé de réception

Par ma signature, je reconnais avoir lu, compris et accepté la politique d'entreprise sur l'usage de l'Intelligence Artificielle.

[Insérer bouton de signature électronique]

—