Nexlor.fr

Charte d’usage de l’intelligence artificielle

Document personnalisable - modèle interne

Organisation	[Nom de l’organisation]
Version	[v1.0]
Date d’entrée en vigueur	[Date]
Responsable	[Nom / Fonction]
Périmètre	[Toute l’organisation / services / filiales]

Accélérer l’usage de l’IA, tout en protégeant les données, les personnes et la confiance.

Sommaire

1. Objet de la charte

Cette charte définit les règles d’usage de l’intelligence artificielle au sein de [Nom de l’organisation].

Elle vise à permettre une utilisation utile, responsable et maîtrisée des outils d’IA, tout en protégeant les données, les personnes, les clients, les partenaires, la propriété intellectuelle et la réputation de l’organisation.

Elle s’applique à tout usage d’outils d’IA, qu’ils soient gratuits, payants, intégrés à des logiciels existants ou développés spécifiquement pour l’organisation.

2. Principes directeurs

- **Utilité professionnelle -** L’IA doit améliorer la qualité du travail, gagner du temps, faciliter l’analyse, stimuler la créativité ou renforcer le service rendu.
- **Responsabilité humaine -** Les décisions importantes restent sous la responsabilité d’une personne identifiée. L’IA assiste, mais ne remplace pas le jugement humain.
- **Protection des données -** Les informations confidentielles, personnelles, sensibles ou stratégiques ne doivent pas être saisies dans un outil d’IA non autorisé.
- **Transparence -** Lorsque l’usage de l’IA a un impact significatif, il doit pouvoir être expliqué.
- **Fiabilité et vérification -** Les résultats produits par l’IA doivent être vérifiés avant utilisation, notamment lorsqu’ils concernent des faits, chiffres, règles juridiques, éléments financiers, techniques ou commerciaux.
- **Équité et non-discrimination -** L’IA ne doit pas être utilisée d’une manière susceptible de produire ou renforcer des discriminations.
- **Sécurité -** Les usages de l’IA doivent respecter les règles internes de cybersécurité, de gestion des accès, de confidentialité et de conformité.

3. Utilisateurs concernés

La présente charte s’applique à l’ensemble des collaborateurs, dirigeants, managers, alternants, stagiaires, intérimaires, prestataires, consultants et partenaires ayant accès aux informations ou systèmes de l’organisation.

4. Usages autorisés

- **Production et amélioration de contenus -** Rédiger un premier brouillon, reformuler un texte, corriger l’orthographe, préparer une synthèse, adapter un message à une cible ou générer des idées de plans et supports.
- **Analyse et aide à la décision -** Structurer une réflexion, comparer des options, identifier des risques, préparer une grille d’analyse ou résumer des documents internes avec un outil validé.
- **Productivité individuelle -** Préparer une réunion, organiser des notes, transformer un compte rendu en plan d’action, créer des modèles de mails ou des check-lists.
- **Développement, informatique et automatisation -** Assister l’écriture de code, expliquer une erreur, documenter un script, générer des tests ou proposer des automatisations simples. Tout code IA doit être relu, testé et validé avant mise en production.

5. Usages interdits

- **Données confidentielles dans un outil non autorisé -** Exemples : données clients, données RH, informations financières non publiques, contrats, prix, marges, secrets d’affaires, codes sources sensibles, identifiants, mots de passe.

- **Données personnelles sensibles -** Exemples : données de santé, opinions politiques, données biométriques, vie privée, données concernant des mineurs.
- **Décision automatisée significative -** Laisser l’IA prendre seule une décision en recrutement, sanction, évaluation individuelle, accès à un service, notation ou décision commerciale sensible est interdit.
- **Contenu trompeur -** Faux avis, fausse identité, deepfake non signalé, manipulation d’image ou de son sans transparence.
- **Contournement des règles de sécurité -** Générer du code malveillant, chercher à contourner des accès ou automatiser des actions non autorisées.
- **Plagiat ou violation de propriété intellectuelle -** Les contenus générés doivent être utilisés avec discernement et vérifiés avant diffusion externe.
- **Résultat IA présenté comme vérité vérifiée -** Toute information factuelle importante doit être contrôlée auprès d’une source fiable.

6. Classification des données et règles d’usage

Niveau	Type de données	Usage avec IA
Public	Informations déjà publiques : site web, brochures, communiqués publiés.	Autorisé
Interne	Informations de travail non sensibles : notes générales, procédures internes non critiques.	Autorisé avec outil validé
Confidentiel	Données clients, contrats, prix, marges, stratégie, documents commerciaux ou financiers.	Interdit sauf outil explicitement autorisé
Sensible	Données personnelles sensibles, secrets d’affaires, sécurité informatique, informations réglementées.	Interdit sauf cadre spécifique validé par [DPO / RSSI / Direction]

Règle simple : en cas de doute sur la sensibilité d’une information, ne pas la saisir dans un outil d’IA et demander validation à [référent IA / DPO / RSSI / manager].

7. Outils autorisés

Outil	Usage autorisé	Niveau de données autorisé	Responsable
[Nom de l’outil 1]	[Rédaction, synthèse, analyse]	[Public / Interne / Confidentiel]	[Nom / Service]
[Nom de l’outil 2]	[Code, support client, automatisation]	[Public / Interne]	[Nom / Service]
[Nom de l’outil 3]	[À compléter]	[À compléter]	[À compléter]

L’utilisation d’un nouvel outil d’IA non listé doit faire l’objet d’une validation préalable par [Direction / DSI / DPO / RSSI / Comité IA].

8. Règles de validation des résultats

Avant d’utiliser ou de diffuser un résultat produit avec l’aide de l’IA, l’utilisateur doit relire le contenu, vérifier les informations factuelles, contrôler les chiffres, dates, noms, références et sources, s’assurer que le contenu respecte les règles internes, la loi et les engagements contractuels, puis adapter le résultat au contexte réel de l’organisation.

Pour les contenus à fort enjeu - juridique, financier, RH, commercial, technique, sécurité ou communication externe - une validation par une personne compétente est obligatoire.

9. Transparence et mention de l’usage de l’IA

L’usage de l’IA doit être mentionné lorsque le contenu est diffusé à l’extérieur et que l’IA a joué un rôle significatif, lorsqu’une image, voix, vidéo ou simulation générée peut être confondue avec un contenu réel, lorsque le client ou le contrat l’exige, ou lorsque l’usage de l’IA influence fortement une analyse.

Formulation possible : « Ce document a été préparé avec l’assistance d’un outil d’intelligence artificielle, puis relu, corrigé et validé par [Nom / Fonction]. »

10. Propriété intellectuelle

Les utilisateurs doivent veiller à ne pas copier dans un outil d’IA des contenus protégés sans autorisation, ni demander la reproduction d’un style, d’une marque ou d’une œuvre protégée d’une manière susceptible de créer une confusion.

Les livrables produits avec l’aide de l’IA dans un cadre professionnel appartiennent à [Nom de l’organisation], sous réserve des règles contractuelles applicables et des conditions d’utilisation des outils concernés.

11. Cybersécurité

Il est interdit de saisir dans un outil d’IA des mots de passe, clés API, jetons d’accès, informations d’architecture critique, vulnérabilités non corrigées ou informations permettant de compromettre un système.

Tout incident, doute ou usage inapproprié doit être signalé à [RSSI / DSI / Référent sécurité] dans les meilleurs délais.

12. Ressources humaines et management

L’IA peut aider à structurer des documents RH ou managériaux, mais elle ne doit pas être utilisée seule pour sélectionner un candidat, évaluer un collaborateur, prendre une décision disciplinaire, décider d’une rémunération, établir un classement individuel automatisé ou analyser des données personnelles de collaborateurs sans cadre validé.

Toute utilisation de l’IA en matière RH doit respecter les règles internes, le droit applicable, la confidentialité et les principes de non-discrimination.

13. Relation client et communication externe

Lorsqu’elle est utilisée dans la relation client ou la communication externe, l’IA ne doit jamais diffuser d’information non vérifiée, promettre ce que l’organisation ne peut pas tenir ou masquer l’usage de l’IA lorsque la transparence est nécessaire.

Les contenus commerciaux, contractuels, institutionnels ou de crise doivent être validés par [Direction / Communication / Juridique / Commercial] avant diffusion.

14. Gouvernance de l’IA

Référent IA : [Nom / Fonction]. Référent sécurité : [Nom / Fonction]. Référent données personnelles : [Nom / Fonction]. Comité de pilotage IA : [Composition, si applicable].

Leur rôle est de tenir à jour la liste des outils autorisés, définir les règles d’usage, accompagner les équipes, évaluer les risques, arbitrer les cas sensibles, organiser la formation et suivre les incidents et retours d’expérience.

15. Formation et accompagnement

[Nom de l’organisation] s’engage à accompagner les utilisateurs dans l’appropriation responsable de l’IA : sensibilisation, formations métiers, guides de bonnes pratiques, exemples de prompts autorisés, ateliers d’usage, partage de cas concrets et dispositif de questions-réponses.

16. Bonnes pratiques de rédaction de prompts

Il est recommandé de formuler clairement l’objectif, préciser le contexte sans divulguer de données sensibles, indiquer le format attendu, demander les limites ou incertitudes, demander des sources lorsque des faits sont cités, vérifier les résultats et éviter les prompts contenant des informations confidentielles ou personnelles.

Exemple recommandé : « Aide-moi à structurer un plan de présentation sur [sujet public ou non sensible]. Propose un plan en 5 parties, avec les points clés à vérifier. Ne crée pas de chiffres non sourcés. »

17. Signalement des incidents ou usages à risque

Tout utilisateur doit signaler rapidement une fuite potentielle de données, un contenu généré faux, discriminatoire ou dangereux, un usage non autorisé d’un outil d’IA, un comportement anormal d’un outil ou une suspicion d’atteinte à la sécurité ou à la confidentialité.

Canal de signalement : [adresse email / outil interne / responsable]. Délai attendu : [immédiat / sous 24h / autre]. Aucun utilisateur ne sera sanctionné pour avoir signalé de bonne foi un risque ou une erreur liée à l’usage de l’IA.

18. Contrôle et conformité

[Nom de l’organisation] peut procéder à des contrôles raisonnables afin de vérifier le respect de la présente charte, dans le respect du droit applicable, des règles internes et des droits des personnes.

Le non-respect de la charte peut entraîner un rappel des règles, une restriction d’accès à certains outils, une formation complémentaire, des mesures disciplinaires en cas de manquement grave ou répété, ou toute autre mesure prévue par les règles internes et la réglementation applicable.

19. Mise à jour de la charte

La présente charte est révisée au minimum [une fois par an / tous les six mois / selon besoin], ou plus fréquemment en cas d’évolution réglementaire, de nouvel outil déployé, d’incident significatif, de retour d’expérience important ou d’évolution des usages métiers.

20. Engagement de l’utilisateur

Champ	À compléter
Nom	[Nom de l’utilisateur]
Fonction	[Fonction]
Date	[Date]
Signature	[Signature]

Annexe 1 - Grille simple d’aide à la décision

Question	Si oui	Si non
Les données sont-elles publiques ou non sensibles ?	Usage possible	Demander validation
L’outil est-il autorisé par l’organisation ?	Usage possible	Ne pas utiliser
Le résultat sera-t-il vérifié par une personne ?	Usage possible	Ne pas diffuser
Le sujet touche-t-il au juridique, financier, RH, sécurité ou client sensible ?	Validation renforcée	Usage standard possible
Le contenu peut-il avoir un impact sur une personne ou un client ?	Transparence et validation nécessaires	Usage possible avec relecture

Annexe 2 - Exemples d’usages par service

Service	Usages possibles	Points de vigilance
Direction	Synthèse, préparation de notes, analyse de scénarios	Données stratégiques et confidentialité
Commercial	Emails, argumentaires, préparation de rendez-vous	Données clients, prix, promesses commerciales
Marketing	Idées de campagnes, contenus, reformulations	Droits d’auteur, image de marque, transparence
RH	Trames d’entretien, fiches de poste, communication interne	Non-discrimination, données personnelles
Finance	Structuration d’analyses, explication de concepts	Chiffres, données confidentielles, validation humaine
Juridique	Aide à la lecture ou structuration de documents	Validation obligatoire par un expert
Informatique	Aide au code, documentation, tests	Sécurité, revue de code, secrets techniques
Support client	Préparation de réponses, synthèse de demandes	Confidentialité client, exactitude des réponses

Annexe 3 - Version courte à afficher en interne

1. Je n’entre pas de données confidentielles ou personnelles sensibles dans un outil non autorisé.
2. Je vérifie toujours les réponses importantes produites par l’IA.
3. Je garde la responsabilité de mes décisions et de mes livrables.
4. Je ne laisse pas l’IA prendre seule une décision sur une personne.
5. Je respecte les droits d’auteur, la confidentialité et les règles internes.
6. Je signale tout incident, doute ou usage à risque.
7. En cas de doute, je demande conseil à [référent IA / manager / DSI / DPO].