POLITIQUE D'UTILISATION DES OUTILS D'INTELLIGENCE ARTIFICIELLE (IA) - XANADU

Version : 1.0

Date d'effet : A définir

Périmètre : Ensemble des collaborateurs et prestataires

1. Objectif

L'émergence des outils d'Intelligence Artificielle Générative (ChatGPT, Copilot, Gemini, Claude, Midjourney, etc.) offre des opportunités de productivité pour **XANADU**.

Cependant, leur utilisation présente des risques majeurs en matière de confidentialité, de propriété intellectuelle et de sécurité des données.

Cette politique vise à encadrer l'usage de ces outils afin de protéger le patrimoine informationnel de l'entreprise, tout en permettant l'innovation.

2. Classification des Outils IA

La politique d'utilisation de l'intelligence artificielle au sein de l'organisation repose sur une distinction fondamentale entre les outils dits « Publics » et les solutions « Entreprise ». Les outils grand public, tels que les versions gratuites de ChatGPT ou Google Gemini, présentent un risque majeur de confidentialité car les données saisies sont susceptibles d'être utilisées pour l'entraînement des modèles et doivent donc être considérées comme potentiellement publiques. À l'inverse, les outils professionnels souscrits explicitement par la DSI, comme Copilot for Microsoft 365, garantissent que les données restent confinées dans le périmètre sécurisé de l'entreprise. En conséquence, la règle d'or impose qu'en l'absence d'une licence entreprise fournie par la DSI, tout outil doit être traité comme public et soumis aux restrictions de sécurité maximales.

3. Protection des Données et Confidentialité

L'injection de données sensibles dans des outils d'IA publics est strictement prohibée. Cette interdiction couvre les données personnelles soumises au RGPD, les secrets d'affaires tels que les stratégies commerciales ou contrats non publics, la propriété intellectuelle technique incluant le code source et les clés API, ainsi que les documents internes confidentiels. Si le

recours à l'IA s'avère nécessaire pour traiter une donnée métier, l'utilisateur a l'obligation absolue de procéder au préalable à une anonymisation irréversible. Cette démarche implique le remplacement des entités nommées par des termes génériques — « Entreprise A » pour XANADU ou « Client X » pour un client — et le masquage des valeurs chiffrées réelles par des ordres de grandeur. Par exemple, il est interdit de demander la rédaction d'une relance pour une facture précise citant le nom du client et le montant exact ; la demande doit être formulée de manière générique pour une prestation indéfinie.

4. Génération de Code et Développement

Dans le cadre des activités de développement informatique, l'utilisation de l'IA pour la génération de scripts est autorisée uniquement à des fins d'aide syntaxique ou pour la création de fonctions génériques. Il est formellement interdit de soumettre aux modèles d'IA des blocs de code propriétaires contenant de la logique métier critique de XANADU. De plus, tout code produit par une intelligence artificielle doit impérativement faire l'objet d'un audit ligne par ligne par un humain avant son intégration ou son exécution, l'IA étant susceptible d'introduire des failles de sécurité ou des références à des dépendances malveillantes.

5. Responsabilité et Vérification

L'utilisateur demeure seul et unique responsable du contenu produit à l'aide d'outils d'intelligence artificielle. Compte tenu de la propension de ces systèmes à « halluciner » ou inventer des faits, une vérification rigoureuse est obligatoire : tout texte, image ou code généré doit être relu et validé par l'humain avant toute diffusion. Par ailleurs, dans un souci de transparence, l'utilisation de l'IA pour la réalisation de livrables formels ou de rapports clients doit être explicitement mentionnée si elle constitue une part substantielle du travail fourni.

6. Sécurité Technique

Sur le plan technique, l'installation d'extensions de navigateur liées à l'IA est interdite sans la validation expresse de la DSI, ces plugins disposant souvent d'un accès total au contenu des pages visitées, y compris l'intranet ou la messagerie. Il est également rappelé que l'utilisation d'outils d'IA à des fins malveillantes, telles que le contournement de sécurités, la création de malwares ou la conception de campagnes de phishing, constitue un motif de licenciement immédiat.

7. Sanctions

Le non-respect des règles d'anonymisation et de confidentialité énoncées dans cette charte est considéré comme une faute grave. Ces manquements exposent l'utilisateur à des sanctions disciplinaires pouvant aller jusqu'au licenciement, sans préjudice d'éventuelles poursuites pénales en cas de violation du secret commercial ou de non-conformité avérée à la réglementation sur la protection des données personnelles.

J'atteste avoir pris connaissance de la présente politique et m'engage à l'appliquer.

Lu et approuvé.

Nom et Prénom : _____

Date : _____ / _____ / _____

Signature :