

nVisionIT

Politique d'utilisation responsable de l'IA : résumé

Version 2.0 de la politique, en vigueur depuis juillet 2026 · Résumé publié en septembre 2026 · www.nvisionit.mu/responsible-ai.html

L'IA assiste. Les humains assument.

nVisionIT dispose d'une politique d'utilisation responsable de l'IA qui encadre tout recours à l'IA dans une mission client, de l'assistant de codage à l'outil agentique. Elle est portée par les administrateurs, approuvée par la directrice générale, revue tous les six mois, et appliquée via l'approbation des outils, la classification des données et un relecteur humain nommé sur chaque livrable. Ce document en est le résumé. La politique complète est destinée aux clients et nous vous l'enverrons sur demande.

Huit engagements qui s'appliquent à chaque mission

Notre programme est aligné sur le Microsoft Responsible AI Standard, l'ISO/IEC 42001 pour les systèmes de management de l'IA, le NIST AI Risk Management Framework et les principes de gouvernance de la technologie et de l'information du King V Report on Corporate Governance, et s'interprète de manière cohérente avec eux.

- **Redevabilité.** Nous restons pleinement responsables de tout système d'IA utilisé dans votre environnement. Des personnes relisent, vérifient et approuvent chaque production générée par l'IA.
- **Équité.** Des processus structurés pour réduire les biais dans le choix des modèles, la rédaction des invites, le traitement des données et l'évaluation des productions.
- **Inclusion.** Les conceptions et interfaces assistées par l'IA sont contrôlées avant livraison pour une accessibilité au moins conforme à WCAG 2.2 AA.
- **Confidentialité.** Minimisation des données, finalité déterminée, consentement, traitement sécurisé et aucune exposition de données confidentielles à des plateformes d'IA externes sans votre accord écrit, au titre de la POPIA et de la DPA mauricienne.
- **Transparence.** Vous avez une visibilité claire sur le rôle de l'IA dans votre mission, sur la manière dont les productions sont générées et validées, et sur les endroits où l'IA a été utilisée dans un livrable.
- **Supervision humaine.** Lorsque l'IA éclaire de façon déterminante une décision produisant des effets juridiques ou comparables sur une personne, un humain compétent prend cette décision ou la réexamine réellement au préalable. Les personnes concernées peuvent demander une revue humaine.
- **Sécurité.** Les processus faisant appel à l'IA sont résilients, gouvernés et protégés contre les usages abusifs, la manipulation et les fuites.
- **Validité.** Tout élément généré par l'IA est contrôlé, testé et vérifié quant à son exactitude et à sa pertinence métier avant d'entrer dans un livrable.

La règle d'exposition zéro

Aucune donnée confidentielle, réglementée, personnelle ou appartenant au client ne peut être soumise à une plateforme d'IA externe sans accord contractuel, sans que la plateforme réponde à vos exigences de sécurité et sans approbation écrite explicite. Il n'existe aucune voie informelle pour contourner cette règle.

Ce que nos équipes n'ont pas le droit de faire

- Soumettre des données de clients, de citoyens, confidentielles ou de tiers à un outil d'IA public sans approbation explicite.
- Livrer du code généré par l'IA sans relecture par un ingénieur, sans tests et sans validation nominative, ou déployer du code non validé dans votre environnement.
- Utiliser l'IA d'une manière qui enfreint la loi, un contrat, des exigences de confidentialité ou des normes sectorielles.
- Produire des contenus trompeurs, frauduleux ou mensongers.

Outils agentiques : une IA qui agit d'elle-même

Les outils agentiques planifient, génèrent, testent, itèrent et exécutent seuls des travaux en plusieurs étapes. Ils comportent plus de risques qu'un assistant de codage : ils font donc l'objet de contrôles supplémentaires.

- **Uniquement avec votre accord écrit.** Les outils agentiques ne sont déployés dans un environnement client que lorsque cela a été explicitement convenu avec vous par écrit. Il n'y a pas de cas par défaut.
- **Jamais raccordés à des systèmes en production sans autorisation.** Ils ne sont jamais raccordés à des systèmes de production ni à des entrepôts de données contenant des informations personnelles ou confidentielles sans votre autorisation écrite et sans une revue de sécurité validée par notre responsable ingénierie.
- **Même relecture, mêmes points de contrôle.** Tout ce qu'un outil agentique produit pour un livrable passe par la même relecture humaine, la même validation et les mêmes points de contrôle qualité que toute autre production assistée par l'IA.
- **Vous pouvez demander à quoi il a eu accès.** Vous pouvez demander le détail de tout outil agentique utilisé sur votre mission, y compris l'étendue des accès qui lui ont été accordés et les contrôles qui lui ont été appliqués.

Vous savez où l'IA a été utilisée

Nous fournissons une déclaration IA client standard chaque fois que l'IA a produit plus qu'un contenu accessoire dans un livrable, par exemple un document d'expression de besoins, un dossier d'architecture de solution, une spécification ou une conception. Elle n'attend pas que vous la demandiez. Elle indique quels outils d'IA ont été utilisés et leur statut d'approbation dans notre registre ; les contrôles appliqués, y compris la relecture humaine, les points de contrôle qualité, l'analyse de sécurité et la règle d'exposition zéro ; la façon dont vos données ont été protégées pendant les travaux ; et la chaîne de responsabilité humaine, c'est-à-dire qui a relu, qui a approuvé et qui en répond.

Qui l'applique, et comment

- **Supervision du conseil et de la direction.** Conformément à King V, notre organe de gouvernance répond de la gouvernance de l'IA, de l'information et de la technologie. La directrice générale approuve les modifications importantes de la politique une fois celle-ci en vigueur.
- **Un registre d'outils gouverné.** Seuls les outils inscrits à notre registre approuvé peuvent être utilisés sur des travaux clients. Chaque entrée consigne la posture de sécurité, les licences, la localisation des données, le niveau de risque, le fait que l'éditeur entraîne ou non ses modèles sur vos données, les cas d'usage approuvés et la date d'approbation.
- **Une responsabilité humaine nommée.** Chaque artefact généré par l'IA qui vous est remis est approuvé par un ingénieur ou un consultant nommé, versionné avec un marquage de provenance, et validé au regard de notre Definition of Done.
- **Surveillance continue.** Nous examinons, à une cadence définie, la performance des modèles et la qualité des productions, les risques de sécurité émergents liés à l'outillage d'IA, la conformité au titre de la POPIA et de la DPA mauricienne, ainsi que l'efficacité des contrôles eux-mêmes.

Incidents et révision

Tout incident lié à l'IA, suspecté ou confirmé, y compris une fuite de données, une production erronée, un contenu préjudiciable ou un accès non autorisé, est immédiatement escaladé en vue d'être contenu et, le cas échéant, notifié au client. Nous enquêtons selon notre protocole de violation POPIA, ou selon le protocole de la DPA mauricienne lorsque des personnes concernées résidant à l'Île Maurice sont impliquées, ce qui inclut la notification au Data Protection Office dans les 72 heures lorsque cela est possible. Vous pouvez demander un rapport d'incident écrit une fois l'enquête close.

La politique est revue tous les six mois, et plus tôt si l'environnement réglementaire évolue, si vos exigences contractuelles changent, si une nouvelle capacité d'IA introduit un risque que la politique en vigueur ne couvre pas, ou si un incident révèle une lacune.

Demandez-nous la politique complète. La politique complète d'utilisation responsable de l'IA est destinée aux clients. Nous vous l'enverrons, accompagnée du modèle de déclaration IA client, des entrées du registre d'outils et des éléments de preuve de sécurité pertinents pour votre mission : info@nvisionit.co.za.