

CHECKLIST

Sécurité des usages de l'IA

Contrôles à conduire avant et pendant l'usage d'outils d'IA générative

La présente liste ordonne les contrôles de sécurité propres aux outils d'IA générative : comptes, données, documents traités, extensions, actions automatisées et incidents. Elle complète la politique de sécurité de l'organisation sans s'y substituer.

1. Comptes et accès

- ☐ Recenser les comptes donnant accès à des outils d'IA, y compris les comptes personnels utilisés pour le travail.
- ☐ Activer l'authentification à deux facteurs sur chaque compte.
- ☐ Rattacher les comptes professionnels à l'organisation et non à des adresses personnelles.
- ☐ Retirer les accès lors du départ d'un collaborateur.

2. Données

- ☐ Définir les données interdites de saisie dans un outil grand public et les diffuser aux utilisateurs.
- ☐ Vérifier, pour chaque outil, l'utilisation des échanges pour l'entraînement, la relecture humaine et la durée de conservation.
- ☐ Désactiver l'utilisation des échanges pour l'amélioration des modèles lorsque l'outil le permet.
- ☐ Réserver les données personnelles et confidentielles aux offres régies par un contrat de traitement.

3. Documents et consignes dissimulées

- ☐ Traiter les documents, pages web et courriels soumis à un outil comme une matière à analyser, non comme des consignes.
- ☐ Ne pas soumettre à un outil disposant de droits d'action des documents d'origine inconnue.
- ☐ Contrôler les liens et pièces jointes produits par un outil avant de les ouvrir ou de les transmettre.

4. Extensions, connecteurs et actions automatisées

- ☐ Soumettre à autorisation l'installation d'extensions de navigateur et d'applications d'IA.
- ☐ Limiter les connecteurs (messagerie, stockage, agenda) aux seuls accès nécessaires.
- ☐ Exiger une validation humaine avant toute action à effet externe : envoi, publication, paiement, suppression.
- ☐ Conserver une trace des actions exécutées par un outil automatisé.

5. Incidents

- ☐ Désigner la personne à qui signaler une saisie accidentelle, une fuite ou un contenu erroné diffusé.

Document d'information générale ; il ne constitue ni une consultation juridique ni un avis sur une situation particulière. Les références aux textes sont à vérifier dans leur rédaction en vigueur à la date d'utilisation.

Cabinet de conseil non inscrit au barreau ; aucune représentation devant les juridictions ni acte réservé aux professions réglementées du droit.

- ☐ Consigner chaque incident : date, outil, données en cause, mesures prises.
- ☐ Examiner, en cas de données personnelles en cause, les obligations découlant de la loi n° 09-08.
- ☐ Examiner, pour les entités qui y sont soumises, les obligations de déclaration prévues par la loi n° 05-20.

Références

- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le dahir n° 1-09-15 du 22 safar 1430 (18 février 2009), BO n° 5711 du 23 février 2009 (édition générale) et n° 5714 du 5 mars 2009 (édition de traduction officielle), article 23.
- Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020), BO n° 6904 du 30 juillet 2020 (édition générale), p. 4160, et n° 6906 du 6 août 2020 (édition de traduction officielle), articles 8, 14, 30 et 33.
- OWASP, « LLM01:2025 Prompt Injection », OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm01-prompt-injection/> (page consultée le 21 octobre 2026).
- OWASP, « LLM06:2025 Excessive Agency », OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm062025-excessive-agency/> (page consultée le 21 octobre 2026).