

CHECKLIST

Security of AI uses

Controls to be carried out before and during the use of generative AI tools

This list sets out, in order, the security controls specific to generative AI tools: accounts, data, documents processed, extensions, automated actions and incidents. It supplements the organisation's security policy without replacing it.

1. Accounts and access

- ☐ Inventory the accounts giving access to AI tools, including personal accounts used for work.
- ☐ Enable two-factor authentication on each account.
- ☐ Attach business accounts to the organisation and not to personal addresses.
- ☐ Revoke access when a staff member leaves.

2. Data

- ☐ Define the data that must not be entered into a consumer tool and communicate them to users.
- ☐ Verify, for each tool, the use of conversations for training, human review and the retention period.
- ☐ Disable the use of conversations for model improvement where the tool allows it.
- ☐ Reserve personal and confidential data for offerings governed by a data processing agreement.

3. Documents and hidden instructions

- ☐ Treat documents, web pages and emails submitted to a tool as material to be analysed, not as instructions.
- ☐ Do not submit documents of unknown origin to a tool that has rights to take actions.
- ☐ Check links and attachments produced by a tool before opening or forwarding them.

4. Extensions, connectors and automated actions

- ☐ Make the installation of browser extensions and AI applications subject to authorisation.
- ☐ Limit connectors (email, storage, calendar) to the access strictly necessary.
- ☐ Require human validation before any action with external effect: sending, publication, payment, deletion.
- ☐ Keep a record of the actions executed by an automated tool.

5. Incidents

- ☐ Designate the person to whom an accidental entry, a leak or erroneous content disseminated is to be reported.
- ☐ Record each incident: date, tool, data involved, measures taken.
- ☐ Where personal data are involved, examine the obligations arising from Law No. 09-08.

General information document; it constitutes neither legal advice nor an opinion on a particular situation. References to legal texts should be checked against the version in force on the date of use.

Consulting firm not registered with the Bar; no representation before the courts and no act reserved to the regulated legal professions.

- ☐ For the entities subject to it, examine the reporting obligations provided for by Law No. 05-20.

References

- Law No. 09-08 on the protection of individuals with regard to the processing of personal data, promulgated by Dahir No. 1-09-15 of 22 Safar 1430 (18 February 2009), Official Bulletin No. 5711 of 23 February 2009 (general edition) and No. 5714 of 5 March 2009 (official translation edition), Article 23.
- Law No. 05-20 on cybersecurity, promulgated by Dahir No. 1-20-69 of 4 Hija 1441 (25 July 2020), Official Bulletin No. 6904 of 30 July 2020 (general edition), p. 4160, and No. 6906 of 6 August 2020 (official translation edition), Articles 8, 14, 30 and 33.
- OWASP, “LLM01:2025 Prompt Injection”, OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm01-prompt-injection/> (accessed on 21 October 2026).
- OWASP, “LLM06:2025 Excessive Agency”, OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm062025-excessive-agency/> (accessed on 21 October 2026).