NL-Q · FICHE-MÉMO

Donner à une IA l'accès à vos données : le moindre accès en pratique

Ce que l'accès apporte.
Un assistant branché sur vos dossiers, votre base ou votre messagerie répond avec vos chiffres et vos documents, pas avec des généralités.

Ce qu'il ouvre.
Tout ce que l'assistant peut ouvrir, une erreur ou un texte piégé peut le lui faire lire, modifier ou envoyer ailleurs.

Ce que contient la fiche.
Six gestes à demander à votre prestataire ou à faire vous-même, sans jargon, puis huit questions pour vérifier.

Pour les dirigeants et responsables de TPE et PME, non développeurs, qui branchent un assistant IA sur leurs données

Édition du 19/11/2026 · NLQ

01 Donnez-lui un compte à lui

Brancher l'assistant avec votre propre compte est le plus rapide, et le plus risqué : il voit alors tout ce que vous voyez et peut faire tout ce que vous faites. L'OWASP cite ce cas parmi les permissions excessives : un module censé lire les documents d'une personne qui se connecte avec un compte capable d'ouvrir ceux de tout le monde.

Un compte réservé à l'assistant.
Par exemple « assistant-ia@example.com ». Il n'appartient à personne et ne sert qu'à lui.

Un mot de passe à lui.
Long, différent de tous les autres et rangé dans un gestionnaire de mots de passe, comme le recommande Cybermalveillance.gouv.fr.

Un compte par assistant.
Deux outils, deux comptes. Le jour où il faut savoir qui a fait quoi, le journal répond (ANSSI R29).

Double authentification côté administrateur.
Le compte qui crée et règle celui de l'assistant est protégé par un second facteur, partout où le service le propose.

02 Commencez en lecture seule

Presque tous les premiers usages consistent à lire : répondre à une question, résumer un dossier, retrouver un chiffre. L'OWASP donne deux exemples. Un assistant qui conseille des achats n'a besoin que de lire la table des produits, sans pouvoir ajouter, modifier ou supprimer. Un assistant qui résume des mails n'a besoin que de lire la boîte, pas d'envoyer.

Rien	Lire un dossier	Lire tout	Modifier	Administrer
l'outil n'est pas branché	le bon départ	rarement utile	au cas par cas	jamais

← MOINS DE RISQUE — PLUS DE RISQUE →

La phrase à demander.
« Un compte pour l'assistant, en lecture seule, sur tel dossier ou telle table, et rien d'autre. » Faites-la écrire dans le devis ou le compte rendu.

La vérification.
Avec le compte de l'assistant, essayez de renommer un fichier d'essai ou de modifier une ligne de test. Si ça passe, ce n'est pas de la lecture seule.

L'écriture plus tard.
Si un jour l'assistant doit modifier ou envoyer, on l'ajoute pour une action précise, avec votre validation avant chaque envoi.

03 Ouvrez un dossier, pas tout le disque

L'ANSSI parle de « besoin d'en connaître » : n'ouvrir que ce qui sert à la tâche (R8). En pratique, on part de la question à laquelle l'assistant doit répondre, et on n'ouvre que les dossiers ou les tables qui contiennent la réponse.

L'ASSISTANT DOIT RÉPONDRE À…	ON OUVRE	ON LAISSE FERMÉ
« Où en est ce chantier ? »	Le dossier du chantier en cours	Les autres clients, la comptabilité
« Quel stock reste-t-il ? »	Les tables Produits et Stocks	Clients, Factures, Fournisseurs
« Que dit le contrat type ? »	Le dossier Modèles de contrats	Les contrats signés, nominatifs

Un dossier « partagé avec l'assistant ».
On y copie ce qui doit être lu. Ce qui n'y est pas, l'assistant ne le voit pas.

Les données sensibles à part.
Santé, dossiers du personnel, coordonnées bancaires : hors du périmètre, sauf décision écrite et motivée.

La liste écrite.
Une ligne par dossier ou table ouverte, avec la date et la personne qui l'a décidé. C'est elle qu'on relira chaque mois.

04 Donnez une clé qui expire

Pour se connecter, l'assistant reçoit souvent une clé : un code d'accès, un jeton, un mot de passe d'application. Une clé sans date de fin reste valable des mois après la fin du projet. La spécification du protocole MCP recommande des jetons de courte durée pour limiter l'effet d'une fuite.

Une date de fin dès la création.
Si l'outil le permet, fixez une durée courte, et renouvelez-la si l'usage continue.

Un seul endroit pour la ranger.
Le gestionnaire de mots de passe, jamais un mail, un tableur partagé ou un pense-bête (Cybermalveillance.gouv.fr).

Une clé par outil.
Si une clé fuit, on la remplace sans couper tous les autres branchements.

Nouvelle clé au départ d'un prestataire.
Quiconque a vu la clé ne doit plus pouvoir s'en servir après la fin de sa mission.

05 Sachez qui coupe, et comment

Le jour où l'assistant fait quelque chose d'inattendu, ou qu'une clé circule, la question n'est plus technique. Qui a le droit de couper, et en combien de temps ? L'ANSSI recommande aussi que l'activité puisse continuer sans l'assistant (R15).

Un nom et un suppléant.
Écrits en tête de la procédure, avec leur numéro.

La procédure en trois lignes.
Désactiver le compte de l'assistant ; révoquer sa clé ; prévenir l'équipe et le prestataire.

Un essai à blanc.
Coupez une fois, un jour calme, et notez le temps qu'il a fallu. Si la procédure bloque, simplifiez-la.

Le service continue.
Notez comment l'équipe travaille pendant la coupure : les mêmes dossiers, à la main.

06 Revoyez les droits chaque mois

L'ANSSI recommande de vérifier les droits d'un outil d'IA dès son activation, car les réglages par défaut peuvent être trop ouverts, puis de les revoir régulièrement, par exemple tous les mois (R35). Une mise à jour de l'outil peut en effet élargir ce qu'il voit.

Le jour de l'activation.
Regardez ce que l'outil ouvre par défaut, avant le premier usage, et refermez ce qui ne sert pas.

Une revue par mois.
La liste écrite, comparée à ce que l'outil ouvre réellement.

Après chaque mise à jour.
Nouvelle fonction ou nouveau connecteur : on relit les droits.

Ce qui ne sert plus, on le retire.
L'OWASP cite le cas d'un module essayé puis abandonné, mais toujours branché.

Comment savoir si c'est en place

Huit questions fermées. Chaque « non » renvoie à un geste de la fiche.

- [ ] L'assistant a-t-il un compte à lui, qui n'est celui de personne ?
- [ ] Existe-t-il une liste écrite des dossiers et tables ouverts ?
- [ ] La clé d'accès a-t-elle une date de fin ?
- [ ] Deux personnes savent-elles couper l'accès sans attendre le prestataire ?
- [ ] Avez-vous essayé de modifier un fichier de test avec ce compte, sans succès ?
- [ ] Les données sensibles sont-elles hors de cette liste ?
- [ ] Savez-vous où elle est rangée, et qui l'a vue ?
- [ ] La dernière revue des droits date-t-elle de moins d'un mois ?

VOTRE PROCHAINE ÉTAPE

Venez avec la liste de ce que votre assistant peut ouvrir aujourd'hui : on regarde ensemble ce qu'on peut lui retirer sans rien perdre.

Réserver un échange gratuit

www.nl-q.com/rendez-vous/

Sources et portée

Toutes les sources ont été ouvertes le 19/11/2026.

- OWASP Gen AI Security Project, *LLM06:2025 Excessive Agency* : permissions excessives, exemples de la table des produits et de la messagerie en lecture seule, modules abandonnés mais toujours branchés. genai.owasp.org/llmrisk/llm062025-excessive-agency/
- ANSSI, guide ANSSI-PA-102 *Recommandations de sécurité pour un système d'IA générative*, version 1.0 du 29/04/2024 : R8, R15, R29, R35. Recommandations sans caractère normatif. messervices.cyber.gouv.fr
- Cybermalveillance.gouv.fr, *Les mots de passe* : un mot de passe par service, gestionnaire, double authentification. cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
- Spécification MCP 2026-07-28, *Authorization — Security Considerations* : jetons d'accès de courte durée. modelcontextprotocol.io/specification/2026-07-28/basic/authorization/security-considerations

Portée : cette fiche ne traite pas des obligations liées aux données personnelles, pour lesquelles le texte et l'autorité compétente font foi. L'adresse du compte et les exemples du tableau sont fictifs.

Édité par NLQ — NL-Q (www.nl-q.com), avec le soutien d'ALMA, sponsor. Édition du 19/11/2026. Exemples fictifs ; ce qui est dit des textes cités vient des sources datées ci-dessus.