

Sécuriser les accès, mots de passe, exports et données clients

La protection des données clients ne repose pas sur un seul mot de passe. Elle combine profils KWISATZ, comptes système, contrôle des exports, accès distants sécurisés, sauvegardes protégées, journalisation et procédure d'incident.

Fiche : SEC-DAT-001 **Public :** direction, administrateurs, DPO, responsables informatiques et support

Risque : critique **Catégorie :** Clients, comptes et protection des données

Mise à jour : 6 août 2026

Réponse directe

Activez des **profils KWISATZ nominatifs**, réservez **SUPERVISEUR** à l'administration, appliquez le moindre privilège et retirez immédiatement les accès des personnes qui changent de fonction ou quittent l'entreprise. Ne comptez pas uniquement sur le mot de passe interne : sécurisez aussi Windows, le serveur, le VPN, la télémaintenance et les sauvegardes. Les exports clients doivent être autorisés, minimisés, chiffrés, transmis par un canal sûr, enregistrés dans un registre et supprimés après usage. Aucune autorisation native universelle dédiée uniquement à l'export des clients ni authentification multifacteur intégrée n'est confirmée dans la documentation fournie.

Conseil technicien général

Conseil technicien — Avant toute modification, créez une sauvegarde exploitable, relevez les réglages existants et testez sur un dossier ou une caisse de recette. Modifiez un seul réglage à la fois, consignez le résultat et faites valider les changements sensibles par un technicien KWISATZ.

Sommaire

1. Repères de version
2. Licence et disponibilité

3. Protection des données
4. Périmètre à protéger
5. Principe du moindre privilège
6. Profils d'utilisateurs KWISATZ
7. Profils, vendeurs et comptes Windows
8. Paramètre -PROFIL
9. Politique de mots de passe
10. Authentification multifacteur
11. Verrouillage et sessions
12. Contrôler les exports
13. Minimiser un export client
14. Registre d'export
15. Stocker et transmettre un export
16. Exports vers Excel et CSV
17. Sauvegardes et données clients
18. Accès réseau et distant
19. Secrets techniques et API
20. Journalisation et audit
21. Données clients : collecte et minimisation
22. Prospection et campagnes
23. Durées de conservation
24. Droits des personnes
25. Sous-traitants et prestataires
26. Départ ou changement de poste
27. Incident ou violation de données
28. Rançongiciel et vol de sauvegarde
29. Plan de contrôle trimestriel
30. Plan de test
31. Actions à éviter
32. Compatibilité documentée
33. Diagnostic rapide
34. Résultat attendu
35. Sources documentaires

1. Repères de version

Les références de version ci-dessous sont conservées comme repères documentaires. Les menus, options et comportements doivent être contrôlés sur la version et la sérialisation réellement installées ; une évolution plus récente peut avoir modifié le fonctionnement.

2. Licence et disponibilité

La dépendance de licence mentionnée dans ce document provient des sources. Sa disponibilité peut varier selon la version, la sérialisation, le partenaire ou l'installation ; faites-la valider techniquement avant de modifier l'environnement.

Conseil technicien — Vérifiez la disponibilité selon la version, la sérialisation, le partenaire et l'installation. Relevez la licence actuelle et faites valider toute évolution avant déploiement.

3. Protection des données

Protection des données — Limitez les données exportées au strict nécessaire, protégez les fichiers et restreignez les accès. Supprimez les copies devenues inutiles, respectez les oppositions et désabonnements, et n'imprimez pas de données sensibles sans nécessité opérationnelle. Une carte, un code-barres ou un identifiant visible ne constitue pas à lui seul une preuve d'identité forte.

4. Périmètre à protéger

Actif	Exemples	Risque
Accès KWISATZ	Profils, vendeurs, SUPERVISEUR, automates.	Consultation ou modification non autorisée.
Accès Windows	Session locale, serveur, TSE, partage réseau.	Contournement des droits applicatifs.
Données clients	Identité, coordonnées, historique, fidélité, comptes.	Divulgence, fraude, prospection illicite.
Exports	Excel, CSV, PDF, états, fichiers comptables.	Copie massive hors contrôle.
Sauvegardes	KWZ, ZIP, répertoires synchronisés, cloud.	Extraction de la totalité du dossier.
Accès distants	VPN, TSE, TeamViewer, poste distant moteur de données.	Intrusion depuis Internet.
Secrets techniques	Mots de passe, jetons, identifiants API.	Prise de contrôle d'un service.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

5. Principe du moindre privilège

Chaque personne doit pouvoir accéder uniquement aux fonctions et données nécessaires à son activité.

- Créer des profils par rôle et non un profil unique pour toute l'entreprise.
- Limiter les menus Clients, Comptabilité, Imports/Exports et Administration.
- Réserver la gestion des profils au SUPERVISEUR.
- Réviser régulièrement les habilitations.
- Désactiver immédiatement les accès devenus inutiles.
- Documenter les exceptions temporaires.

Un profil partagé empêche d'identifier avec certitude l'auteur d'une consultation, d'une modification ou d'un export.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

6. Profils d'utilisateurs KWISATZ

Le menu **Démarrage > Profils d'utilisateurs** associe un nom, un mot de passe et des droits d'accès aux fonctions principales.

- Le profil SUPERVISEUR existe par défaut.
- Tant qu'il reste seul, la gestion des utilisateurs n'est pas activée.
- La création d'un second profil active la sélection d'un utilisateur au lancement.
- La gestion des profils devient inaccessible aux profils non SUPERVISEUR.

Protégez le profil SUPERVISEUR et conservez un accès de secours sous contrôle de la direction. Ne l'utilisez pas comme compte quotidien.

7. Profils, vendeurs et comptes Windows

Niveau	Fonction	Bonne pratique
Compte Windows	Accès au poste et aux fichiers.	Compte nominatif, session verrouillée.
Profil KWISATZ	Accès aux menus et fonctions de gestion.	Droits adaptés au rôle.
Vendeur	Autorisations et traçabilité en Vente directe.	Code et mot de passe individuels.
Compte technique	Service, automate, API ou sauvegarde.	Secret distinct, droits minimaux, usage documenté.

Ces niveaux se complètent. Un profil KWISATZ limité ne protège pas les fichiers si le compte Windows donne un accès direct au serveur ou aux sauvegardes.

Conseil technicien — Sauvegardez, relevez les réglages existants et testez cette modification sur un dossier ou une caisse de recette. Ne changez qu'un paramètre à la fois et faites valider les réglages sensibles par un technicien KWISATZ.

8. Paramètre -PROFIL

Le paramètre `-PROFIL=NOM_UTILISATEUR` peut présélectionner un profil au lancement.

Si le profil ne possède pas de mot de passe, l'ouverture peut être immédiate. N'utilisez pas cette configuration pour un poste exposé, un profil sensible ou un accès distant.

9. Politique de mots de passe

- Utiliser un secret unique par personne et par service.
- Préférer une phrase de passe longue et difficile à deviner.
- Interdire les mots de passe par défaut ou évidents.
- Ne pas partager un mot de passe par courriel ou messagerie avec le fichier protégé.
- Utiliser un gestionnaire de mots de passe approuvé.
- Changer immédiatement un secret compromis.
- Ne pas imposer un changement périodique sans motif lorsqu'il conduit à des secrets faibles ; changer lors d'un risque ou d'un départ.

Les limites historiques de certains mots de passe vendeurs KWISATZ ne constituent pas une politique moderne suffisante pour protéger un serveur ou un accès Internet.

10. Authentification multifacteur

Aucune MFA native n'est confirmée dans KWISATZ. Activez-la sur les couches qui le permettent :

- compte Microsoft ou fournisseur d'identité ;
- VPN ;
- TSE/RDS ou passerelle distante ;

- outil de télémaintenance ;
- console cloud ;
- messagerie qui reçoit les exports ;
- portail de sauvegarde.

Les comptes administrateurs et les accès distants doivent être prioritaires pour la MFA.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

11. Verrouillage et sessions

- Configurer le verrouillage automatique de Windows.
- Ne jamais laisser une session SUPERVISEUR ouverte en caisse.
- Fermer la session TSE après intervention.
- Limiter les tentatives de connexion lorsque le système le permet.
- Contrôler les sessions distantes encore actives.
- Éviter les mots de passe mémorisés dans les raccourcis ou scripts lisibles.

Conseil technicien — Sauvegardez, relevez les réglages existants et testez cette modification sur un dossier ou une caisse de recette. Ne changez qu'un paramètre à la fois et faites valider les réglages sensibles par un technicien KWISATZ.

12. Contrôler les exports

KWISATZ documente des exports depuis les listes écrans et des exports avancés de documents. Aucune autorisation native universelle dédiée uniquement à l'export des clients n'est confirmée.

Limiter l'accès à la liste Clients ne garantit pas que toutes les autres éditions, statistiques ou interfaces contenant des données clients sont bloquées. Réalisez un test fonctionnel par profil.

Avant l'export	Question
Finalité	Pourquoi les données sont-elles nécessaires ?
Autorisation	Qui a validé l'opération ?
Périmètre	Quels clients et quelles colonnes sont réellement utiles ?
Destination	Où le fichier sera-t-il stocké et transmis ?
Durée	Quand sera-t-il supprimé ?
Traçabilité	Comment l'opération sera-t-elle enregistrée ?

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

13. Minimiser un export client

1. Filtrer la population strictement nécessaire.
2. Retirer les colonnes non utiles.
3. Éviter les commentaires libres et mémos si la finalité ne les exige pas.
4. Remplacer les identifiants directs par un code lorsque possible.
5. Contrôler un échantillon avant génération complète.
6. Vérifier que les filtres restent actifs dans le fichier final.

Un export de « tous les clients » par défaut est rarement proportionné à une demande ciblée.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

14. Registre d'export

Champ	Exemple
Date et heure	20/07/2026 15:20.
Demandeur	Responsable marketing.
Opérateur	Profil et personne ayant généré le fichier.
Finalité	Rappel clients ayant une commande en cours.
Périmètre	42 clients, nom, téléphone et numéro de commande.
Format	CSV chiffré.
Destinataire	Prestataire contractuel identifié.
Suppression prévue	Date et responsable.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

15. Stocker et transmettre un export

- Éviter le Bureau, Téléchargements et les clés USB non chiffrées.
- Utiliser un répertoire limité aux personnes autorisées.
- Chiffrer le fichier ou l'archive avec une solution approuvée.
- Transmettre le secret par un canal différent.
- Éviter les liens publics et les partages sans expiration.
- Supprimer les copies locales, temporaires et de messagerie après usage.
- Demander une confirmation de suppression au sous-traitant.

Un fichier CSV ou Excel n'est pas protégé simplement parce qu'il se trouve dans une archive ZIP.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

16. Exports vers Excel et CSV

- Forcer les codes en format texte pour éviter les pertes de zéros.
- Contrôler les séparateurs et l'encodage.
- Ne pas ajouter de colonnes contenant des secrets ou mots de passe.
- Supprimer les formules ou liens externes inutiles.
- Vérifier les fichiers temporaires créés par le tableur.
- Fermer le fichier avant sa suppression sécurisée du poste.

17. Sauvegardes et données clients

Une sauvegarde contient potentiellement l'intégralité des clients, historiques, documents, tickets et réglages.

- Limiter les droits sur le dossier de sauvegarde.
- Utiliser un compte technique dédié.
- Conserver une copie hors ligne ou immuable lorsque possible.
- Chiffrer les supports transportables.
- Contrôler la synchronisation cloud et la rotation.
- Tester une restauration isolée.
- Documenter les personnes pouvant télécharger une archive.

La purge automatique d'anciennes sauvegardes synchronisées peut supprimer les copies locales et cloud. Vérifiez la politique avant de l'activer.

Conseil technicien — Sauvegardez et relevez les chemins, droits, identifiants techniques et fréquences existants. Testez les échanges sur un périmètre limité et faites valider les changements d'interface par un technicien KWISATZ.

18. Accès réseau et distant

- Privilégier un VPN avec authentification forte.
- Limiter les accès par adresse IP lorsque possible.

- Ne pas exposer directement moteur de données sur Internet sans architecture sécurisée.
- Protéger TSE, RDS, TeamViewer et consoles cloud par MFA.
- Utiliser des comptes nominatifs pour la maintenance.
- Fermer les accès temporaires après intervention.
- Journaliser les connexions administratives.

Les ports moteur de données `12005` et `12006` documentés pour les postes distants ne doivent pas être ouverts sans VPN, filtrage et analyse de risque.

Conseil technicien — Sauvegardez et relevez les chemins, droits, identifiants techniques et fréquences existants. Testez les échanges sur un périmètre limité et faites valider les changements d'interface par un technicien KWISATZ.

19. Secrets techniques et API

- Ne pas stocker un `client_secret` en clair dans un fichier accessible.
- Restreindre les droits Windows sur les fichiers de configuration.
- Masquer les jetons et mots de passe dans les journaux.
- Renouveler les secrets selon la procédure du fournisseur.
- Utiliser un compte ou client technique distinct par environnement.
- Révoquer immédiatement un secret exposé.

20. Journalisation et audit

La journalisation sert à détecter les accès anormaux, comprendre un incident et établir une chronologie.

- Journaliser les connexions administratives.
- Conserver les logs Windows, VPN, TSE, sauvegardes et interfaces.
- Surveiller les exports massifs et téléchargements inhabituels.
- Protéger les logs contre la modification.
- Limiter leur durée de conservation à ce qui est nécessaire.
- Informer les utilisateurs selon les règles internes applicables.

La piste d'audit KWISATZ ou un journal technique ne doit jamais être supprimé pour masquer une anomalie ou gagner de l'espace.

21. Données clients : collecte et minimisation

- Collecter seulement les informations nécessaires à la finalité.
- Éviter les informations sensibles dans les commentaires libres.
- Rendre obligatoires uniquement les champs réellement nécessaires.
- Vérifier l'exactitude des coordonnées.
- Informer les clients de l'usage de leurs données.
- Distinguer gestion contractuelle, fidélité et prospection.
- Conserver la preuve du consentement lorsqu'il constitue la base utilisée.

22. Prospection et campagnes

Contrôle	Action
Finalité	Distinguer information de service et prospection commerciale.
Base légale	Valider la règle applicable au canal et au type de client.
Opposition	Exclure les personnes opposées à la prospection.
Prestataire	Encadrer contractuellement l'usage et la suppression.
Export	Limiter les colonnes au strict besoin de la campagne.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

23. Durées de conservation

KWISATZ ne peut pas décider seul de la durée légale ou métier applicable à chaque donnée.

1. Définir une durée par finalité.
2. Distinguer base active et archivage intermédiaire.
3. Conserver les pièces soumises à une obligation légale.
4. Supprimer ou anonymiser les données devenues inutiles lorsqu'aucune obligation ne s'y oppose.
5. Documenter les exceptions et contentieux.

Ne supprimez pas directement une fiche client liée à des factures, règlements ou pièces comptables sans vérifier les obligations de conservation et les liens du dossier.

24. Droits des personnes

Demande	Traitement interne
Accès	Identifier les données et documents concernant la personne.
Rectification	Corriger les informations inexactes.
Opposition	Bloquer les usages concernés, notamment la prospection lorsque applicable.
Effacement	Analyser obligations légales, contrats et pièces liées.
Limitation	Geler certains usages pendant l'analyse.
Portabilité	Préparer les données couvertes dans un format structuré lorsque le droit s'applique.

Une demande RGPD doit être gérée par la procédure du responsable de traitement, pas par une suppression improvisée dans la base.

25. Sous-traitants et prestataires

- Identifier hébergeur, mainteneur, routeur SMS, emailing, cloud et plateforme de facturation.
- Définir les instructions, la confidentialité et la sécurité par contrat.
- Limiter les comptes et données accessibles.
- Exiger la notification rapide des incidents.
- Contrôler la restitution et la suppression en fin de contrat.
- Documenter les transferts de données hors Espace économique européen lorsqu'ils existent.

Conseil technicien — Sauvegardez et relevez les chemins, droits, identifiants techniques et fréquences existants. Testez les échanges sur un périmètre limité et faites valider les changements d'interface par un technicien KWISATZ.

26. Départ ou changement de poste

1. Désactiver le profil KWISATZ.
2. Désactiver le vendeur ou changer son secret.
3. Fermer le compte Windows.
4. Révoquer VPN, TSE, TeamViewer et comptes cloud.
5. Récupérer badges, clés Dallas et supports.
6. Changer les secrets partagés connus de la personne.
7. Contrôler ses exports et partages encore actifs.
8. Conserver la traçabilité nécessaire.

27. Incident ou violation de données

Une violation peut être une perte, une destruction, une altération, une divulgation ou un accès non autorisé à des données personnelles.

1. Contenir l'incident sans détruire les preuves.
2. Déconnecter ou isoler le poste compromis si nécessaire.
3. Révoquer les comptes et secrets exposés.
4. Identifier les données, personnes, période et destinataires concernés.
5. Conserver journaux, copies de fichiers et chronologie.
6. Informer immédiatement la direction et le référent RGPD.
7. Évaluer le risque pour les personnes.
8. Documenter la violation dans tous les cas.
9. Notifier l'autorité compétente si le risque l'exige, si possible dans les 72 heures.
10. Informer les personnes lorsque le risque est élevé, sauf exception applicable.

Le délai se compte à partir de la prise de connaissance de la violation, pas de la fin de l'enquête technique.

28. Rançongiciel et vol de sauvegarde

- Ne pas reconnecter immédiatement les sauvegardes saines au système compromis.
- Préserver au moins une copie hors ligne.
- Changer les secrets depuis un poste sain.
- Contrôler les exports et sauvegardes exfiltrés, pas seulement les fichiers chiffrés.

- Restaurer dans un environnement isolé.
- Vérifier l'intégrité des données avant la reprise.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

29. Plan de contrôle trimestriel

Contrôle	Attendu
Profils KWISATZ	Comptes nominatifs et droits cohérents.
SUPERVISEUR	Usage exceptionnel et secret protégé.
Comptes Windows	Aucun compte ancien ou partagé injustifié.
Accès distants	MFA, VPN, comptes actifs et journaux contrôlés.
Exports	Registre, finalité et suppression vérifiés.
Sauvegardes	Accès restreints et restauration testée.
Sous-traitants	Contrats et comptes techniques à jour.
Incidents	Procédure et contacts testés.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

30. Plan de test

Scénario	Résultat attendu
Profil vendeur	Accès Clients ou Administration refusé si non requis.
Profil gestion	Accès aux clients sans droits superviseur.
Export client	Autorisation et registre exigés par la procédure.
Compte quitté	Accès KWISATZ, Windows et VPN désactivés.
Export chiffré	Ouverture impossible sans secret transmis séparément.
Sauvegarde	Téléchargement limité aux comptes habilités.
Accès distant	MFA et journalisation fonctionnelles.
Incident simulé	Chronologie, contacts et analyse du délai de 72 heures maîtrisés.

Conseil technicien — Sauvegardez avant le traitement, conservez les paramètres et le fichier source, puis testez un échantillon sur un dossier de recette. Contrôlez les résultats avant de traiter l'ensemble.

31. Actions à éviter

- Utiliser SUPERVISEUR au quotidien.
- Partager un profil ou un mot de passe entre plusieurs personnes.
- Lancer automatiquement un profil sensible sans mot de passe.
- Exposer directement moteur de données sur Internet sans protection forte.
- Envoyer un CSV client non chiffré par courriel.
- Conserver les exports dans Téléchargements ou sur une clé USB ordinaire.
- Oublier les sauvegardes dans l'inventaire des données.
- Supprimer une fiche liée à des pièces légales sans analyse.
- Effacer les journaux après un incident.
- Attendre la fin de l'enquête avant d'évaluer la notification.

32. Compatibilité documentée

Fonction	Disponibilité documentée	Limite
Profils utilisateurs	Nom, mot de passe et droits principaux.	Gestion réservée à SUPERVISEUR.
- PROFIL	Présélection d'un profil.	Ouverture immédiate si aucun mot de passe.
Exports de listes	Export depuis les listes écrans.	Droit dédié à l'export client non confirmé.
Exports avancés	Documents et états selon les écrans.	Tester chaque profil et chaque liste.
MFA native	Non confirmée.	À assurer par les couches externes.
Sauvegarde cloud	WKW_ARCHIVE_CLOUD et dossier synchronisé.	Accès cloud, chiffrement et purge à contrôler.
Accès distant	- CSD et moteur de données selon licence.	VPN, filtrage et MFA recommandés.

Conseil technicien — Vérifiez la disponibilité selon la version, la sérialisation, le partenaire et l'installation. Relevez la licence actuelle et faites valider toute évolution avant déploiement.

33. Diagnostic rapide

Un utilisateur voit les vendeurs et leurs mots de passe

Contrôlez le profil, l'accès aux grilles annexes, la version et les chemins de sélection rapide. Mettez à jour une version ancienne présentant ce défaut historique.

Un profil peut exporter toute la liste clients

Aucun droit universel dédié n'est confirmé. Limitez son accès à la liste, contrôlez les autres états et appliquez une procédure d'export.

Le paramètre -PROFIL ouvre directement KWISATZ

Le profil ne possède probablement aucun mot de passe. Ajoutez une protection ou retirez la présélection.

Un ancien salarié se connecte encore à distance

Révoquez immédiatement Windows, VPN, TSE, télémaintenance, cloud et secrets partagés.

Un export client a été envoyé sans chiffrement

Demandez sa suppression, identifiez les destinataires, changez le canal et évaluez s'il s'agit d'une violation de données.

Une sauvegarde a été copiée sur un ordinateur personnel

Considérez qu'elle contient potentiellement toutes les données du dossier, récupérez ou effacez la copie et analysez l'incident.

Un fichier protégé et son mot de passe ont été envoyés dans le même courriel

Le chiffrement est pratiquement neutralisé. Révoquez le lien ou le secret et renvoyez par deux canaux distincts.

Une clé API apparaît dans un journal

Révoquez-la, nettoyez les journaux selon une procédure conservant les preuves et activez le masquage des secrets.

Un client demande l'effacement de sa fiche

Analysez les pièces légales, comptes, factures et finalités avant suppression ou anonymisation.

Une fuite est découverte vendredi soir

Le délai d'analyse et de notification ne s'arrête pas le week-end. Activez immédiatement la procédure d'incident.

34. Résultat attendu

Chaque utilisateur dispose d'un compte identifiable et des seuls droits nécessaires. SUPERVISEUR reste protégé, les accès distants utilisent une authentification renforcée, les exports clients sont minimisés, autorisés, chiffrés et tracés, les sauvegardes sont restreintes et restaurables, et les données ne sont conservées que pour une finalité justifiée. Toute violation est contenue, documentée et évaluée immédiatement au regard des obligations de notification.

35. Sources documentaires

- MENUS KWISATZ — profils utilisateurs, activation automatique et gestion réservée à SUPERVISEUR.
- Tutoriels KWISATZ — paramètre `-PROFIL`.
- Suivi de développement — exports depuis les listes et exports avancés.
- Suivi de développement — correction historique d'un contournement d'accès aux grilles annexes.
- Version 3.56 — sauvegardes synchronisées via `WKW_ARCHIVE_CLOUD`.
- CNIL — Guide de la sécurité des données personnelles 2024, habilitations, authentification, journalisation et violations.
- ANSSI — authentification multifacteur, mots de passe et hygiène informatique.
- RGPD — sécurité du traitement et notification des violations.

Documentation KWISATZ. Appliquez le moindre privilège, protégez chaque copie de données et préparez la réponse aux incidents avant qu'ils ne surviennent.

Catégorie : Clients, comptes et protection des données · Mise à jour : 6 août 2026.