

Dossier technique et sécurité VDR

Architecture, contrôles, preuves et responsabilités
pour les revues de sécurité d'entreprise.

Édition 1.7 · 7 octobre 2026

Production : v3.1.0-enterprise.25

VDR, démonstrations et pilotage — livraison signée

Document partageable · Aucune information secrète ou donnée client

Chaque contrôle est décrit avec son périmètre et ses limites. Ce document ne constitue pas une certification ni un engagement contractuel.

Sommaire

1. Périmètre et niveau de preuve
2. Architecture et frontières de confiance
3. Isolation des organisations et des données
4. Rôles administratifs et délégation Partner
5. Authentification, MFA et clés d'accès
6. Durée et révocation des sessions — lot complémentaire
7. Rooms, permissions, groupes et NDA
8. Affichage sécurisé, filigranes et export
9. Chiffrement des objets et gestion des clés
10. Chiffrement de champs et exposition de métadonnées
11. Cartographie du chiffrement et des transports observés
12. Import, antivirus et reprise de transfert
13. Conversion, OCR et recherche documentaire
14. Versions, rédaction et clôture de room
15. Préservation, conservation et confidentialité
16. Audit, intégrité et rapports
17. API et intégrations — lot complémentaire
18. IA et sous-traitance de contenu
19. Notifications et messagerie
20. Livraison logicielle et gestion des vulnérabilités
21. Sauvegardes, restauration et reprise d'activité
22. Surveillance, incidents et responsabilités
23. Résidence, conformité et documents contractuels
24. Limites techniques de référence
25. Matrice de contrôles et preuves
26. Démonstrations clientes, accès temporaires et guide
27. Pilotage institutionnel, cohortes et échéances
28. Annexe : réponses au questionnaire acheteur

Périmètre et niveau de preuve

HiveRoom est une plateforme de salles de données virtuelles et de portails investisseurs. Ce dossier décrit les frontières de confiance, les contrôles applicatifs, les opérations de sécurité et leurs limites. Il est destiné aux équipes de sécurité, aux acheteurs et aux responsables techniques. Date de référence : 7 octobre 2026 ; édition 1.7.

La référence de production de cette édition est v3.1.0-enterprise.25. Le lot de fonctions VDR de la PR runtime n° 35 a passé 326 tests unitaires et une campagne complète de 60 scénarios navigateur en CI, avant une livraison signée enterprise.18. La version enterprise.20 regroupe les démonstrations guidées avec suppression des accès à expiration, le pilotage multi-room, les cohortes, les échéances et la recherche native dans le lecteur protégé. Le candidat enterprise.19 n'a pas été activé : un scan actualisé a demandé la mise à jour de Sharp de 0.35.4 à 0.35.5, intégrée à enterprise.20. Les nombres de tests et de scénarios de ce dernier lot sont indiqués dans ses preuves CI. Les reçus de livraison identifient les images par digest. Les tests applicatifs utilisent des données synthétiques ; ils ne constituent pas un audit indépendant de tous les dossiers clients.

La campagne complète du code livré en enterprise.25 a passé 422 tests unitaires et 78 scénarios navigateur. Les contrôles de TypeScript, lint, design, dépendances, secrets, analyse statique et images runner/migration/processeur sont verts sur le même arbre de source. Les identifiants des campagnes sont conservés dans la provenance de cette édition.

Les preuves internes comprennent les résultats des tests, les reçus de livraison, les vérifications de signatures, les analyses de vulnérabilités et les rapports de restauration. Leur existence permet une revue technique ; elle ne constitue ni une certification, ni un rapport indépendant de pénétration, ni une garantie contractuelle de disponibilité.

Le lot enterprise.21 ajoute les correspondances contextuelles et minimisées, les liens de récupération liés à l'espace, la sélection locale de passages à partir d'une question et des brouillons facultatifs gouvernés. Seuls les lots couverts par le reçu de cette édition sont déclarés livrés.

Le lot enterprise.22 ajoute les webhooks signés et leurs reprises ainsi que les récapitulatifs documentaires quotidiens et hebdomadaires. Aucun endpoint client ni destinataire externe n'a été activé par les tests de cette édition.

Le lot regroupé enterprise.24 ajoute les comités à décisions indépendantes, les politiques de transition et les rapports chiffrés planifiés. Les baux, révisions, révocations et limites ont été qualifiés sur des données synthétiques.

Ce lot regroupé enterprise.24 ajoute les conversations d'équipes acheteurs et les rappels de retard Q&A avec consentement. Un essai local de concurrence synthétique demeure une observation de son environnement et ne fonde pas un engagement de capacité en production.

Le lot enterprise.24 ajoute les adaptateurs de stockage actif chiffré S3/Azure, la conservation documentaire par pays/catégorie et référence de fermeture, ainsi que la revalidation des images après lecture. Le mode cloud nécessite toujours une activation et qualification opérateur sur le fournisseur retenu.

Les fonctions comités/rapports, équipes acheteurs/rappels et stockage/conservation ont été regroupées dans une seule campagne finale et livraison entreprise.24 sur la PR runtime n° 41. Il n'existe pas de déploiement entreprise.23 intermédiaire ; les campagnes locales préparatoires sont distinguées de la campagne complète de l'arbre final.

La référence de cette édition est entreprise.25, qui conserve les fonctions du lot regroupé et corrige le packaging des outils de reprise/rotation. Les preuves de l'échec précédent sont conservées ; seules les preuves de restauration de la version courante sont présentées comme qualifiées.

Sources techniques : docs/ops/2026-10-06-platform-completion-validation.md

Architecture et frontières de confiance

Le plan de contrôle gère les opérateurs Partner, les organisations, les domaines, les modèles de configuration, le provisionnement, les versions et les vérifications de santé. Le runtime héberge les utilisateurs des espaces, les rooms, les documents, les NDA, les demandes d'accès et les opérations investisseurs. Ces applications ont des modèles de données et des responsabilités distincts.

Le runtime utilise Next.js 16, React 19, Prisma 7 et PostgreSQL. Les fichiers téléversés sont conservés dans un stockage applicatif chiffré. Des services spécialisés effectuent le contrôle antivirus, le traitement PDF/Office et l'OCR. Redis et les services de sécurité font partie de la configuration de déploiement ; ils ne doivent pas être exposés comme services publics.

Le navigateur accède au service par HTTPS. Le serveur résout l'espace de travail puis vérifie l'identité, l'appartenance à cet espace et les droits sur la room et le document. Le contenu est déchiffré uniquement dans le chemin serveur autorisé ou dans le processeur requis. Les services externes de messagerie et d'IA sont des frontières supplémentaires soumises à configuration et, pour l'IA, à approbation explicite.

Les modes proposés dans le plan de contrôle comprennent le partage de runtime, une base dédiée et une pile dédiée. L'éligibilité d'un mode ne prouve pas sa mise en service pour un client. La topologie, la région, les réseaux, les volumes et les engagements doivent être vérifiés sur le déploiement commandé.



Flux externes conditionnels : messagerie configurée ; IA explicitement approuvée.

Sources techniques : prisma/schema.prisma ; src/lib/tenant.ts ; src/lib/auth-tenant.ts

Isolation des organisations et des données

Les modèles portant un tenant sont interrogés avec le contexte d'espace résolu. Les memberships et grants ne sont pas déduits d'un identifiant de projet envoyé par le navigateur. Les actions sensibles relisent les droits actuels ; un accès antérieur à une page ne suffit pas à autoriser une mutation ultérieure.

Les relations composites de plusieurs modèles associent tenant, room, document et version, afin de bloquer des références incohérentes entre espaces. Ce mécanisme complète les contrôles applicatifs. Il ne remplace pas l'analyse de toutes les routes ni une isolation matérielle dans un mode partagé. Ce dossier ne revendique pas une politique universelle de Row Level Security PostgreSQL.

Le lot complémentaire ajoute un annuaire d'entreprises, des liens de parties à une transaction et une recherche autorisée. Lier une entreprise à un dossier ne lui accorde aucun accès. La recherche vérifie le rôle, l'état de la room, les permissions et la version actuelle avant de retourner des résultats ; les acteurs dont les droits ne permettent pas le texte ne reçoivent pas d'extraits.

Sources techniques : `src/lib/workspace-rbac.ts` ; `src/lib/room-document-access.ts` ; `src/lib/document-search.ts` ; `prisma/migrations/20261006110000_platform_completion/migration.sql`

Rôles administratifs et délégation Partner

Les rôles de workspace distinguent notamment propriétaire, administrateur, opérateur, auditeur et participant. Les autorisations sur les pages et les API sont contrôlées séparément. Les opérations de clés API, conservation, demandes de confidentialité, configuration sensible et clôture nécessitent un propriétaire humain lorsque le lot complémentaire l'exige.

L'accès Partner utilise une identité technique distincte d'un compte humain. Un ticket aléatoire de 32 octets est stocké sous forme de SHA-256, valable 60 secondes et consommable une seule fois. Le grant délégué expire au bout de 30 minutes et peut être révoqué. Il ne crée pas d'appartenance humaine à l'espace.

Les routes de données d'identité/KYC et les opérations sensibles sont exclues de cette délégation. Un espace exigeant le MFA refuse ce chemin Partner si la délégation ne démontre pas l'assurance requise. Cette restriction est un comportement de sécurité, pas une prise en charge du SSO d'entreprise.

Sources techniques : `src/lib/partner-access.ts` ; `src/lib/workspace-rbac.ts` ; `src/lib/workspace-owner.ts`

Authentification, MFA et clés d'accès

Les mots de passe sont vérifiés avec bcrypt ; le helper de création utilise un coût de 12. L'authentification est soumise aux contrôles de fréquence et au contexte d'hôte/espace. Les identités Partner ne peuvent pas utiliser le chemin de mot de passe humain. Une suspension ou un rejet de compte invalide les requêtes ultérieures selon les contrôles d'authentification.

Le MFA utilise des codes TOTP avec consommation anti-rejeu, des codes de récupération protégés et des secrets chiffrés. L'activation d'une politique obligatoire exige l'enrôlement des membres humains. La suppression d'un MFA est refusée si un espace associé l'exige ; elle nécessite la vérification du mot de passe et d'un code, puis révoque les tokens existants.

Les passkeys utilisent une vérification utilisateur imposée par le chemin WebAuthn. Leur assurance ne vaut pas une intégration SAML/SCIM. Les fournisseurs d'identité, règles d'attribution, provisioning, révocation et scénarios de secours d'entreprise doivent être qualifiés séparément.

Les cookies d'authentification sont configurés Secure en production. L'identité de l'utilisateur, son statut et sa version de token sont relus. Les protections CSRF et d'origine des routes s'ajoutent aux contrôles d'accès ; les secrets, liens de récupération et tickets ne doivent pas être transmis dans des journaux publics.

Les liens de création ou réinitialisation du mot de passe utilisent un jeton aléatoire dont le hash SHA-256 est lié à l'espace. Le même utilisateur membre de deux espaces ne peut pas consommer le lien sur l'autre domaine. Une consommation valide utilise un verrou et une mise à jour atomique, exige un mot de passe de 14 à 128 caractères avec les classes requises, invalide les autres liens et les sessions existantes et écrit son audit dans la même transaction. Les anciens liens non liés à un espace sont invalidés à l'activation de cette version ; une nouvelle émission est nécessaire.

Sources techniques : `auth.ts` ; `src/lib/password.ts` ; `src/lib/mfa.ts` ; `src/lib/mfa-policy.ts` ; `src/lib/http/define-route.ts` ; `src/lib/reset-token.ts` ; `src/app/api/auth/reset-password/route.ts`

Durée et révocation des sessions — lot complémentaire

Le registre serveur de sessions humaines conserve un identifiant opaque, l'utilisateur, l'espace, une expiration fixe à huit heures, une assurance PASSWORD/MFA/PASSKEY/LEGACY, un agent utilisateur borné et une empreinte IP à clé. Un rafraîchissement de token ne prolonge pas la durée depuis l'émission initiale.

L'utilisateur peut consulter et révoquer une session, les autres sessions ou toutes ses sessions. La révocation totale incrémente la version des tokens. Les requêtes suivantes vérifient le registre ; les mutations lentes sensibles réévaluent la session après le travail préparatoire.

Un espace nouvellement soumis au MFA exige une session d'assurance forte. Une ancienne session ou une session créée par mot de passe seul ne devient pas forte du fait d'un changement de politique. Le prochain accès demande une authentification appropriée. L'expiration n'efface pas une copie déjà téléchargée.

Sources techniques : `src/lib/login-sessions.ts` ; `src/app/api/auth/sessions/route.ts` ; `auth.ts`

Rooms, permissions, groupes et NDA

L'accès aux documents dépend du statut du participant, de l'invitation/grant actif, de son expiration, de la room, des règles sur dossiers et fichiers et des permissions d'affichage/téléchargement. Une room privée ne peut pas être révélée par simple connaissance de son slug. Le lot complémentaire dissimule les teasers privés non autorisés et contrôle le cycle PREPARATION/LIVE/LOCKED/CLOSED.

La validation du NDA peut précéder l'ouverture de la data room. Dans le nouveau mode versionné, l'acceptation est liée à une révision et à une empreinte SHA-256 du texte, avec snapshot chiffré et PDF de preuve. Une modification de texte ou d'exigence invalide la dispense offerte par l'ancienne révision. L'approbation d'une demande obsolète est refusée.

Les demandes et preuves de NDA sont protégées contre la réécriture de leur contenu signé. Les changements de statut de revue restent possibles. Les rooms existantes gardent leur mode historique à la migration ; les nouvelles rooms utilisent le mode versionné. Cette différence doit être considérée lors de la reprise d'une transaction existante.

La preuve de consentement applicative et le PDF de NDA ne sont pas présentés comme une signature électronique qualifiée, un horodatage qualifié ou une opinion juridique sur la validité de l'accord.

Le propriétaire humain peut activer explicitement les conversations Q&A d'un groupe de participants. L'auteur doit confirmer le partage ; l'audience d'un fil est immuable et ses suivis héritent de cette audience. Les membres actuels doivent toujours disposer de l'accès room et satisfaire la politique NDA/session. Un membre retiré, y compris l'auteur initial, perd l'accès à la conversation de groupe. Les réponses explicitement publiées en FAQ peuvent être visibles aux autres participants autorisés ; leurs suivis privés, auteurs, brouillons et notes de revue ne sont pas exposés. Les historiques empêchent la suppression d'un groupe : sa désactivation reste disponible.

Sources techniques : [src/lib/room-document-access.ts](#) ; [src/lib/nda-access.ts](#) ; [src/lib/nda-revision.ts](#) ; [src/app/api/nda/sign/route.ts](#) ; [src/lib/qa-audience.ts](#) ; [src/lib/qa-participant.ts](#) ; [src/app/api/questions/route.ts](#)

Affichage sécurisé, filigranes et export

Les aperçus PDF protégés passent par une vérification serveur et ajoutent un filigrane d'identité. Le téléchargement utilise une décision distincte. Un accès de lecture n'autorise pas automatiquement le téléchargement du document source ; les contraintes de rôle, groupe et individu restent applicables.

Les restrictions d'interface d'impression et de téléchargement réduisent les actions disponibles dans le parcours fourni. Elles ne garantissent pas l'impossibilité de capture d'écran, de photographie ni de reconstruction par un utilisateur autorisé. La gestion de droits persistants dans des applications externes nécessite un produit DRM/IRM et une qualification distincts.

Les autorisations et l'expiration agissent sur les accès suivants au service. Une copie préalablement obtenue ne peut pas être révoquée universellement par le runtime. Les accords, le marquage et la gouvernance du destinataire complètent les contrôles techniques.

Les images protégées relisent désormais l'acteur, la version et les permissions après la lecture du stockage et le rendu. Les images KYC doivent correspondre à un enregistrement actuel du même tenant, relu avant restitution. L'accès est enregistré dans un audit durable avant l'émission des octets ; une défaillance d'audit refuse la réponse.

Sources techniques : `src/app/api/preview/[docId]/route.ts` ; `src/lib/watermark.ts` ; `src/lib/room-document-access.ts` ; `src/app/api/files/[...path]/route.ts`

Chiffrement des objets et gestion des clés

Le format HVRMENC3 utilise AES-256-GCM. Chaque objet reçoit une clé de données aléatoire de 32 octets. La clé de données est enveloppée par la clé active du keyring, avec un IV aléatoire de 12 octets et un tag de 16 octets. Le contenu utilise son propre IV/tag et une donnée authentifiée associée au format. L'enveloppe inclut un identifiant de clé.

Une rotation de clé d'enveloppe peut réenvelopper la clé de données sans réécrire le contenu chiffré. La clé précédente doit rester accessible en lecture jusqu'à vérification de tous les objets. Les formats historiques ont des chemins de migration ; la lecture de fichiers en clair nécessite une option explicite et ne constitue pas la posture cible.

Dans le runtime partagé, le keyring d'enveloppe est commun au déploiement. Une clé de données par objet ne signifie pas une clé maîtresse dédiée à chaque tenant, ni du BYOK. La donnée authentifiée du contenu identifie le format ; elle ne constitue pas une liaison cryptographique universelle au tenant. L'isolation des accès demeure applicative et relationnelle. Une séparation de clés par client doit être conçue et qualifiée pour le déploiement demandé.

Les fichiers sont écrits avec des permissions restrictives. Le chiffrement applicatif protège les objets conservés ; il ne prouve pas le chiffrement de tous les volumes ou de toutes les colonnes de la base. Les noms de rooms, métadonnées et relations peuvent rester lisibles pour un administrateur disposant des droits de base de données. La protection du système hôte et des sauvegardes reste essentielle.

Les secrets de production sont indépendants pour l'authentification, le chiffrement des objets, le chiffrement PII, les index de recherche, les codes de récupération et l'intégrité de l'audit. Le chargement par fichiers montés et le keyring permettent la gestion opérationnelle. La procédure d'accès d'urgence, les détenteurs de clés et les approbations de rotation sont à convenir avec l'exploitant.

Le code prend en charge un stockage actif S3 ou Azure Blob via les SDK officiels, avec activation réservée à une configuration opérateur approuvée. Le mode de livraison par défaut demeure LOCAL : aucune qualification d'un compte cloud client n'est déduite de tests synthétiques. Le mode cloud conserve et exige un cache local chiffré ; chaque lecture couverte récupère l'enveloppe distante et compare son empreinte au cache avant déchiffrement. Absence, indisponibilité ou divergence refuse la lecture, sans fallback silencieux. Les écritures requièrent l'acceptation distante avant le cache, avec clés d'objet opaques et namespace propre au déploiement. KYC, staging mobile et parties de transfert conservent leur stockage local séparé. Limite de cinquante et un MiB par enveloppe, trois tentatives et signal d'abandon de quarante-cinq secondes couvrant aussi le flux de réponse. Aucune URL publique, SAS ou URL présignée d'original n'est émise.

Les modes cloud nécessitent une migration des enveloppes existantes et une qualification sur le fournisseur réel, ses régions, politiques de confidentialité, IAM, versions et reprise. Le bootstrap est une simulation par défaut ; son mode opérateur explicite téléverse du ciphertext et vérifie sa restitution. La suppression traite l'objet courant avant son cache ; les versions historiques cloud et les sauvegardes restent distinctes. La rotation met à jour l'enveloppe distante avant le remplacement atomique du cache ; une interruption peut refuser les lectures jusqu'à résolution de la divergence. Cette architecture n'est pas une exploitation sans cache ni une reprise multi-région.

Sources techniques : [src/lib/secure-file.ts](#) ; [docs/ops/secret-management.md](#) ; [src/lib/object-storage.ts](#) ; [scripts/bootstrap-object-storage.ts](#) ; [docs/ops/object-storage.md](#)

Chiffrement de champs et exposition de métadonnées

Les champs sensibles couverts utilisent HVRMP11, AES-256-GCM, un IV aléatoire et une donnée authentifiée propre au champ/contexte. Les narratifs de préservation, demandes de confidentialité, snapshots de NDA, résultats d'analyse et chemins de purge du lot complémentaire utilisent des contextes associés pour empêcher leur substitution.

La recherche d'email peut utiliser un index aveugle HMAC-SHA-256 sur l'email normalisé avec une clé indépendante. Un index aveugle permet des correspondances sans conserver le champ de recherche en clair ; il ne cache pas nécessairement les relations ou toutes les métadonnées présentes ailleurs.

Les informations de sécurité minimisent le contenu lorsque possible : IP d'audit transformée par HMAC, agent utilisateur borné, événements sans narratif confidentiel pour plusieurs nouvelles opérations. Une empreinte IP ne constitue pas une anonymisation irréversible en toutes circonstances. Les autres journaux techniques, routes historiques et politiques de conservation nécessitent une revue propre à la configuration.

Sources techniques : `src/lib/pii-crypto.ts` ; `src/lib/audit-crypto.ts` ; `src/lib/privacy-requests.ts` ; `src/lib/legal-holds.ts`

Cartographie du chiffrement et des transports observés

Cette cartographie distingue le chiffrement applicatif des contenus, le transport et les volumes. Le relevé du 7 octobre 2026 ne consulte que des métadonnées TLS agrégées ; aucune donnée client ni valeur de secret n'est exposée.

Les connexions TCP PostgreSQL observées sur les services du plan de contrôle et du runtime ne négocient pas TLS. Les endpoints internes de préparation documentaire et de rendu PDF utilisent HTTP avec authentification de service sur le réseau Docker. Le réseau privé et les secrets de service limitent l'accès, mais ne constituent pas un chiffrement de transport.

La configuration Redis examinée utilise redis:// sur le réseau interne. Le chiffrement universel des disques, volumes de base, métadonnées, caches ou journaux n'est pas établi par le chiffrement applicatif des objets. Une extension exigeant TLS sur chaque flux interne ou des volumes chiffrés doit être configurée et qualifiée séparément.

Flux ou données	Protection observée	Périmètre / limite
Navigateur → service	HTTPS	Périmètre public, sous réserve de la configuration TLS du domaine
Application → PostgreSQL	TCP interne sans TLS observé	Réseau privé et droits de base ; pas de revendication TLS interne
Application → Redis	redis:// dans la configuration examinée	Contrôle de réseau/secret ; chiffrement de transport non établi
Application → processeur/rendu	HTTP interne authentifié	Sandbox/ressources et authentification ; pas de TLS sur ce flux
Documents couverts et dérivés	AES-256-GCM applicatif	DEK par objet ; keyring partagé, ni BYOK ni KEK par tenant
Profils/identité et narratifs couverts	Chiffrement de champs sélectionnés	Autres métadonnées et relations distinctes
Sauvegardes distantes	Archive chiffrée et transport configuré	Clés et conservation séparées ; exercice documenté
Disques, volumes, caches et logs	Chiffrement universel non établi	À cartographier/qualifier selon la topologie commandée

Sources techniques : src/lib/prisma.ts ; src/lib/document-content.ts ; docker-compose.yml ; docker-compose.secrets.yml

Import, antivirus et reprise de transfert

Les téléversements vérifient la taille, le type déclaré, les extensions prises en charge et les signatures de fichiers lorsque définies. Le chemin sécurisé soumet les octets à ClamAV avant validation finale ; une indisponibilité du scanner obligatoire bloque l'import. Le marqueur de test EICAR est également refusé. Le contrôle de signature seul ne prouve pas l'innocuité du document.

Le lot complémentaire ajoute la reprise de transfert par parties de 1 MiB, jusqu'à 50 MiB par document. Les parties sont chiffrées côté serveur ; les identifiants et chemins sont générés par le serveur. Le fichier final est vérifié par son SHA-256 complet puis par les contrôles de format et antivirus. Une reprise nécessite le même fichier d'origine ; le navigateur ne stocke pas son contenu comme mécanisme de reprise.

Une session d'import expire après 24 heures. Les plafonds sont notamment 20 fichiers ouverts et 512 MiB par compte, 2 GiB par tenant et 1 000 sessions globales. La finalisation utilise un reçu d'import lié à utilisateur/room/requête/empreinte ; une répétition ne crée pas un second document. Les parties incomplètes ne sont pas publiées comme documents valides.

Sources techniques : `src/lib/file-security.ts` ; `src/lib/malware-scanner.ts` ; `src/lib/resumable-import.ts` ; `src/lib/commit-document-import.ts`

Conversion, OCR et recherche documentaire

Les conversions et l'OCR sont délégués à un processeur authentifié et limité en ressources, utilisant des fichiers temporaires et des restrictions de sandbox. Le service n'est pas un navigateur public pouvant librement accéder à des ressources distantes. Les conversions produisent des dérivés ; les documents sources restent distincts.

La préparation automatique est configurable et désactivée par défaut au niveau de l'espace. La file persistante lie tenant, room, document et version. Les baux et tentatives permettent une reprise après un arrêt du worker. Une version devenue obsolète ne doit pas fournir de texte au chemin actuel.

Les limites comprennent 50 MiB par source, 200 pages traitables, jusqu'à 30 pages d'OCR et 512 KiB de texte préparé. La recherche est une recherche bornée sur noms et texte préparé, dans un corpus autorisé. Elle n'est pas présentée comme un index exhaustif illimité ni comme une recherche sémantique globale.

Sources techniques : `src/lib/document-content.ts` ; `src/lib/content-jobs.ts` ; `src/lib/document-search.ts` ; `workers/document-processor/server.mjs`

Versions, rédaction et clôture de room

L'historique conserve les sources/versionnements selon les règles de l'application. Le lot complémentaire compare exactement des lignes de texte dans une limite de 1 200 lignes et 1 MiB cumulé. L'accès à la version archivée et à la version actuelle reste contrôlé ; une limite dépassée provoque un refus explicite.

La rédaction PDF brûle les régions choisies par l'utilisateur dans une nouvelle image de chaque page, puis reconstruit un PDF. Cette reconstruction écarte le texte caché, formulaires, liens et métadonnées de la source. Elle est limitée à 30 pages et 100 régions, avec un rendu borné. L'utilisateur doit sélectionner les régions et vérifier le résultat ; ce mécanisme n'est pas une détection automatique exhaustive de données sensibles.

Le document rédigé devient une nouvelle version en brouillon, avec téléchargement et impression désactivés ; la source d'origine est préservée et les dérivés sont recalculés. Une preuve locale a contrôlé l'absence du secret par extraction native et OCR indépendant ainsi que la conservation du texte visible et de l'original déchiffrable.

L'archive de clôture réservée au propriétaire peut inclure des sources, versions et PDF de NDA, ainsi qu'un index CSV, des manifestes SHA-256 et des données de room. Elle exclut les dossiers KYC, notes privées et secrets. L'archive exportée contient des documents en clair sans le filigrane du viewer : l'interface demande une acceptation explicite. Elle est bornée à 100 sources et 50 MiB, sans résultat silencieusement partiel.

Sources techniques : `src/lib/text-diff.ts` ; `src/lib/document-redaction.ts` ; `workers/document-processor/redact-images.py` ; `src/app/api/admin/documents/closeout/route.ts`

Préservation, conservation et confidentialité

Les legal holds du lot complémentaire ciblent une room ou un document dans l'espace. Leur narratif et leur motif de levée sont chiffrés. Les contraintes applicatives et les triggers de base protègent les originaux, versions et preuves concernées contre suppression, changement de référence et cascade. Une nouvelle version n'est admise qu'avec préservation correcte de l'ancienne source.

La conservation documentaire s'applique aux rooms CLOSED, avec une durée configurée de 1 à 3 650 jours. L'automatisation est inactive par défaut et nécessite une acceptation explicite. Les candidats sous hold sont exclus. Une purge crée d'abord un travail durable chiffré puis supprime le contenu éligible ; le worker vérifie l'absence de référence avant suppression physique du fichier et conserve une preuve de résultat.

Ce moteur ne supprime pas instantanément tous les NDA, audits, sauvegardes ou catégories réglementaires. Sa preuve indique explicitement que les sauvegardes ne sont pas effacées par la purge. Des obligations de préservation, les cycles de sauvegarde et les politiques contractuelles peuvent retarder l'effacement complet.

Les demandes de confidentialité sont des dossiers de revue de compte : accès, correction, effacement, restriction, portabilité et opposition. L'utilisateur consulte ses demandes ; un propriétaire les traite avec réponses et preuves séparées. Les narratifs sont chiffrés et les dossiers finaux deviennent immuables. L'export est limité au compte et aux données couvertes. Il ne constitue pas une promesse d'effacement automatique ni une attestation globale de conformité GDPR.

La politique de conservation de room peut restreindre les suppressions à un pays enregistré et jusqu'à vingt catégories documentaires exactes. Elle peut prendre comme référence la création de la pièce ou la date la plus tardive entre sa création et la fermeture enregistrée de la room. Lorsqu'un filtre est configuré, un pays inconnu ou différent et une catégorie absente ou différente excluent la pièce ; le mode fondé sur la fermeture exige une date enregistrée. Aucun critère manquant n'est interprété comme un droit de suppression. Aucun délai légal n'est déduit du pays. Une révision optimiste protège les sauvegardes et demandes de purge ; room, politique, âge, catégorie et legal holds sont relus sous verrou avant suppression. Réouvrir une room réinitialise sa référence de fermeture. Les rooms historiquement fermées sans preuve de date ne reçoivent pas de date reconstituée. Les politiques NDA, audit, KYC et sauvegardes demeurent séparées de ce périmètre documentaire.

Sources techniques : `src/lib/legal-holds.ts` ; `src/lib/document-retention.ts` ; `src/lib/privacy-requests.ts` ;
`prisma/migrations/20261006093000_legal_holds/migration.sql` ; `src/lib/retention-scope.ts` ;
`prisma/migrations/20261007100000_storage_retention/migration.sql`

Audit, intégrité et rapports

Les événements d'audit enregistrent action, acteur, tenant, cible, détails contrôlés, date, agent utilisateur et empreinte IP lorsque fournis. Une chaîne HMAC relie les entrées par espace ; un verrou transactionnel sérialise la création des maillons. Cela rend vérifiables certaines altérations dans le périmètre de la clé disponible.

La chaîne n'est pas un registre externe infalsifiable, un stockage WORM universel ni un horodatage de tiers. Une compromission des droits de base et de la clé réduit son niveau d'assurance. La fonction historique `auditLog` journalise une erreur sans bloquer l'application ; les nouvelles mutations conséquentes utilisent l'écriture transactionnelle durable lorsque documentée. La couverture exacte doit être examinée par événement.

Les exports CSV/PDF du lot complémentaire sont filtrés et réservés aux rôles autorisés. L'export d'audit CSV est limité à 10 000 événements, le PDF à 2 000 ; les rapports d'activité CSV à 5 000. Les PDF ont des limites de taille/pages et signalent les caractères non pris en charge par la police. Le CSV conserve le texte Unicode. Ces observations ne mesurent pas une intention d'investissement.

Les rapports privés disposent d'une file asynchrone, avec bail de cinq minutes et trois tentatives. Les fenêtres portent sur un à quatre-vingt-dix jours UTC complets. Les plans quotidiens ou hebdomadaires appartiennent au propriétaire humain et expirent au plus après quatre-vingt-dix jours ; les dates manquées ne sont pas rattrapées. Les droits du créateur, du lecteur et du plan sont relus avant et après génération et avant restitution. L'artefact est chiffré, associé à une empreinte SHA-256, limité à vingt MiB et supprimé à son échéance par le traitement de fond. L'expiration de l'artefact ne supprime pas les enregistrements source. L'audit exclut narratifs, IP et agents utilisateur ; CSV audit dix mille lignes, PDF deux mille lignes et deux cents pages. Le PDF utilise une police standard : certains caractères non représentables sont remplacés ; le CSV conserve Unicode. Ces limites refusent une exportation partielle silencieuse.

Sources techniques : `src/lib/audit.ts` ; `src/lib/audit-crypto.ts` ; `src/lib/report-pdf.ts` ; `src/app/api/admin/audit/export/route.ts` ; `src/lib/scheduled-reports.ts` ; `src/app/api/admin/reports/jobs/route.ts`

API et intégrations — lot complémentaire

Les clés API utilisent 32 octets aléatoires et ne sont affichées qu'à la création ; seul le SHA-256 est enregistré. Leur création nécessite un propriétaire humain. Chaque clé lie un espace, des rooms explicites et des scopes de lecture de métadonnées. Les endpoints rooms/documents ne retournent pas les octets sources, chemins de stockage ni données KYC.

L'expiration est comprise entre 1 et 90 jours ; les quotas journaliers configurables vont de 10 à 100 000 requêtes. Les plafonds incluent 20 clés actives et 50 rooms par clé. La révocation et les droits actuels sont vérifiés côté serveur. Une description OpenAPI est disponible pour ces endpoints limités ; ce périmètre n'est pas un écosystème universel d'intégrations.

Les webhooks sortants de métadonnées sont réservés au propriétaire humain et désactivés dans les démonstrations. Chaque endpoint exige une approbation explicite du destinataire et des événements : activité d'audit avec ID/action/date sans acteur ou narratif, ou publication documentaire avec IDs/version pour les rooms sélectionnées. URL et secret de signature sont chiffrés avec une donnée authentifiée liée au tenant et à l'endpoint. Vingt endpoints actifs et cent historiques sont admis ; une rotation du secret invalide les événements en attente de l'ancienne génération.

Une file transactionnelle conserve les événements avec bail, six essais, reprises et identifiant stable pour déduplication du destinataire. Le HMAC-SHA256 couvre la date fraîche et les octets JSON exacts. Avant chaque connexion, la résolution est refaite, les adresses non publiques sont refusées et l'IPv4 validée est épinglée ; SNI, Host et certificat restent liés au domaine d'origine. HTTPS avec certificat vérifié, port 443, quinze secondes, sans redirection, huit KiB de réponse. La révocation est relue après DNS. Une requête déjà commencée ne peut pas être rappelée ; HTTP 2xx confirme seulement l'acceptation par le destinataire. La limite de dix mille événements en attente refuse l'opération d'origine au lieu de perdre silencieusement une souscription couverte. Ce pont générique n'est pas un connecteur ECM/DMS ni une fédération SAML/SCIM qualifiés.

Sources techniques : `src/lib/integration-api.ts` ; `src/app/api/v1/openapi/route.ts` ; `src/app/api/v1/documents/route.ts` ; `src/lib/webhook-transport.ts` ; `src/lib/webhook-queue.ts` ; `src/lib/webhook-dispatch.ts` ; `src/app/api/admin/settings/api-keys/webhooks/route.ts`

IA et sous-traitance de contenu

L'IA du runtime est prévue pour le fournisseur Anthropic configuré dans le code. L'espace doit activer le fournisseur et approuver les catégories ; le texte documentaire et le NDA exigent l'autorisation de contenu confidentiel. Un événement d'egress est écrit durablement avant l'appel, sans journaliser le contenu transmis. Sans configuration et approbation requises, le chemin refuse le traitement.

Le lot complémentaire détecte localement certains motifs sensibles, notamment email, cartes validées par Luhn et secrets typiques, avec un nombre de résultats borné. Ces motifs sont indicatifs. Les résumés/catégorisations proposés exigent des citations exactes de l'extrait autorisé ; les propositions chiffrées sont liées à la version et soumises à validation humaine.

L'assistant s'appuie sur au plus huit documents choisis, jusqu'à 6 000 caractères par source et 48 000 au total. Une réponse fondée sur ces extraits ne constitue pas une revue complète de toutes les pièces ni une opinion juridique. Les limites de corpus, l'incertitude et le besoin de revue doivent être conservés dans le parcours client.

Les conditions de traitement, conservation fournisseur, région, contrats et usage secondaire doivent être confirmés avec le fournisseur retenu. Ce dossier ne promet pas une absence de conservation ou d'entraînement sur la base de la seule intégration. Les tests locaux de cette édition n'ont transmis aucun document client à un fournisseur d'IA.

La recherche avec une question utilise une sélection locale lexicale de passages exacts dans le texte préparé, avec au plus 200 documents et 30 MiB de texte par room. Les offsets sont liés au contenu original et les extraits sont présentés avant toute IA. Ce mécanisme n'est pas un moteur vectoriel ou une compréhension sémantique exhaustive. Un brouillon facultatif nécessite une approbation du fournisseur et des catégories document/question, relue avant et après l'appel. Les citations doivent appartenir aux sources autorisées et les versions/dérivés sont relus ; aucun brouillon n'est conservé automatiquement.

Sources techniques : `src/lib/ai-policy.ts` ; `src/lib/ai-governance.ts` ; `src/lib/document-intelligence.ts` ; `src/app/api/admin/documents/assistant/route.ts` ; `src/lib/question-retrieval.ts` ; `src/app/api/admin/documents/question/route.ts`

Notifications et messagerie

La messagerie externe dépend d'un fournisseur configuré, actuellement Resend dans le chemin concerné. Le lot complémentaire conserve une outbox durable et idempotente par destinataire/document/version, avec bail de deux minutes, jusqu'à six tentatives et contrôle des préférences et droits au moment de l'envoi.

Les alertes documentaires utilisent un objet et un corps génériques sans nom de pièce ou contenu confidentiel. Le fournisseur reçoit cependant l'adresse du destinataire et les données nécessaires à la livraison. Des identifiants absents ou des valeurs de test ne produisent pas une fausse preuve d'envoi réussi.

Les notifications historiques couvertes par le module email sont désormais rendues avec la marque et un domaine HTTPS vérifié appartenant à l'espace. Les messages d'inscription, NDA, questions et demandes commerciales emploient un contenu générique et n'incorporent plus les noms, textes de question/réponse ou narratifs confidentiels. Les messages de création/récupération de mot de passe et d'invitation transmettent toutefois le jeton temporaire nécessaire et l'adresse destinataire au fournisseur. Cette minimisation ne constitue pas une affirmation sur des campagnes marketing distinctes.

Le statut de livraison du job signifie que le fournisseur a accepté la demande ; il ne prouve pas l'arrivée dans la boîte de réception, la lecture ou l'absence de classement en spam. Les alertes marketing et campagnes plus larges ont un périmètre différent. Aucun message externe réel n'a été envoyé par les tests de ce lot.

Les préférences proposent immédiat, quotidien ou hebdomadaire. Le quotidien devient éligible à minuit UTC suivant et l'hebdomadaire au lundi UTC suivant. Les lots sont limités à deux cents mises à jour, avec identifiant durable utilisé pour l'idempotence fournisseur. Chaque pièce/version et chaque accès sont relus ; un document modifié ou un grant révoqué est exclu. Désactiver les courriels annule les éléments en attente ; un message déjà remis ne peut pas être rappelé. Les dates et les préférences ne prouvent pas la délivrabilité réelle du domaine expéditeur.

Les rappels de retard Q&A sont désactivés par défaut et requièrent une politique approuvée par le propriétaire ainsi qu'un consentement individuel. Le traitement quotidien UTC cible l'affectataire ou les relecteurs de l'étape actuelle du comité, avec relecture de leur rôle, des préférences, du délai et de la révision source. Chaque destinataire/question/jour possède un identifiant durable ; six essais, un bail de deux minutes et une expiration après vingt-quatre heures bornent la file. Aucun texte de question, réponse, nom ou raison métier n'est envoyé. La désactivation annule les essais en attente ; une requête commencée ne peut pas être rappelée. L'acceptation du fournisseur ne prouve pas la réception en boîte de messagerie.

Sources techniques : `src/lib/email.ts` ; `src/lib/mail-outbox.ts` ; `src/app/api/notifications/preferences/route.ts` ; `src/lib/mail-context.ts` ; `src/lib/mail-renderer.ts` ; `src/lib/document-digest.ts` ; `prisma/migrations/20261007070000_enterprise_connectivity/migration.sql` ; `src/lib/qa-reminders.ts` ; `src/app/api/admin/settings/qa-reminders/route.ts`

Livraison logicielle et gestion des vulnérabilités

Les branches suivent spécification, plan et PR. La CI exécute TypeScript strict, ESLint, règles de design, tests unitaires et parcours Playwright sur base jetable. Les gates sécurité incluent Semgrep strict, analyse de secrets, revue de licences/dépendances et Trivy sur dépôt et images de production.

Les images runtime, migration et processeur sont identifiées par digest et signées. Le déploiement contrôlé vérifie les signatures et réalise un déploiement progressif avec contrôles de santé. La preuve de version lie l'artefact au code qualifié. Un retour d'image n'annule pas automatiquement une migration de base ; la compatibilité des migrations et les sauvegardes sont nécessaires.

Un scan sans vulnérabilité corrigible au seuil appliqué n'établit pas l'absence de vulnérabilités inconnues ni la réussite d'un pentest indépendant. Les règles, bases de signatures et dépendances évoluent. Les revues, correctifs et observations restent nécessaires après livraison.

La restauration du lot enterprise.24 a validé les bases et les fichiers chiffrés, puis identifié une dépendance de source absente dans l'outil opérateur de rotation. Le correctif enterprise.25 embarque les modules de stockage nécessaires et le script de bootstrap. Un contrôle de l'image construite charge réellement ces modules, effectue un aller-retour de chiffrement sur une donnée synthétique et exécute le bootstrap en simulation sans réseau ni identifiant de production. Ce contrôle ne qualifie aucun fournisseur cloud réel. La restauration courante citée par cette édition a été réalisée après la livraison de cette image corrigée.

Sources techniques : [.github/workflows/ci.yml](#) ; [.github/workflows/security.yml](#) ; [.github/workflows/release-image.yml](#) ; [ops/delivery/deliver.py](#) ; [Dockerfile](#) ; [scripts/ci/check-runner-recovery.mjs](#) ; [ops/validation/2026-10-07-recovery-packaging.md](#)

Sauvegardes, restauration et reprise d'activité

La configuration Hiveroom dispose de sauvegardes chiffrées distantes et d'une procédure de restauration isolée. L'exercice courant du 7 octobre 2026 est postérieur à la livraison enterprise.25 et utilise son image de runtime exacte ; il qualifie donc le schéma livré, au-delà de l'exercice historique du 6 octobre. Il couvre l'archive distante, sa vérification, les bases et fichiers, les contraintes et les parcours applicatifs. Sa durée n'est pas un RTO de service.

Le rapport courant a validé 21 tables et 24952 lignes pour le plan de contrôle, 91 tables et 742 lignes pour le runtime, 156 fichiers de manifeste et 10 fichiers uploadés déchiffrés. Les parcours ont couvert authentification, isolation, NDA, KYC, refus de documents révoqués, antivirus et rotation/retour de clés sans modification de production. Les ressources temporaires ont été supprimées. Fin d'exercice : 2026-10-07T13:10:33.821358+00:00.

Une restauration hebdomadaire est installée pour le samedi vers 02:20 UTC avec une fenêtre de délai, et une vérification de fraîcheur est prévue toutes les cinq minutes avec seuil de neuf jours. La périodicité de la sauvegarde et sa conservation effective doivent être documentées pour le déploiement et la période contractuelle ; ce dossier ne réutilise pas les anciens calendriers Alcazar comme preuve Hiveroom.

La perte complète de l'hôte, un standby dans un autre domaine de panne, la récupération indépendante des clés, le basculement DNS et la reprise des écritures ne sont pas établis par cette restauration sur l'infrastructure actuelle. Les objectifs de runbook RPO 24 h/RTO 4 h restent des cibles à qualifier ; ils ne sont pas garantis ici. La réplication multi-région et le PITR ne sont pas déclarés opérationnels.

Sources techniques : docs/ops/disaster-recovery.md

Surveillance, incidents et responsabilités

Les contrôles de santé et services de sécurité fournissent des signaux techniques. Les incidents doivent être qualifiés en tenant compte du service touché, du périmètre client, de l'intégrité des données et des droits d'accès. La collecte technique ne remplace pas une astreinte humaine.

Les horaires de prise en charge, canaux de notification, délai d'escalade, délai de notification d'une violation, obligations contractuelles et responsables de communication doivent figurer dans le contrat/runbook de service. Ce dossier n'affirme pas un service humain 24/7 en l'absence de preuve d'équipe et de contrat.

L'exploitant gère durcissement hôte, réseaux, clés, sauvegardes, mises à jour, alertes et réponse. Le client attribue et révisé les accès, vérifie les NDA et le contenu, contrôle les exports et fournit ses obligations de conservation. La plateforme applique les contrôles applicatifs décrits dans la version effectivement livrée.

Sources techniques : [src/lib/security-v5.ts](#) ; [docs/ops/secret-management.md](#)

Résidence, conformité et documents contractuels

La résidence doit être définie pour bases, fichiers, sauvegardes, journaux, accès administratifs et transferts vers les sous-traitants. Une région de configuration ou une option commerciale ne prouve pas le lieu de tous les traitements. Le pays, l'hébergeur et les sous-traitants finaux doivent être confirmés dans l'annexe de service.

Les catégories externes identifiées sont hébergement/stockage, messagerie, IA lorsqu'activée, domaines/TLS et éventuels outils d'observabilité. La liste de sous-traitants, leurs localisations et accords de traitement doit être validée pour le contrat, sans conclure que chaque catégorie traite tous les fichiers.

SOC 2 et ISO 27001 ne sont pas déclarés obtenus. Un programme de contrôles internes, des tests logiciels et un audit de code ne remplacent pas une évaluation indépendante. Les obligations GDPR, DPA, mécanismes de transferts, délais de réponse, registres et politiques documentaires nécessitent une analyse juridique et organisationnelle.

Avant commande, demander l'annexe de déploiement, la liste de sous-traitants, le DPA, les politiques de conservation, les procédures de réponse et les engagements de support/reprise. Les prestations d'intégration d'identité, régions supplémentaires et DRM doivent être chiffrées et qualifiées comme projets distincts.

Sources techniques : [src/lib/ai-policy.ts](#) ; [src/lib/email.ts](#) ; [docs/ops/disaster-recovery.md](#)

Limites techniques de référence

Ces limites sont des garde-fous de la version du lot complémentaire, pas des capacités contractuelles, ni une preuve de performance sous charge. Une qualification de volumétrie et de concurrence reste nécessaire pour un engagement dimensionné.

Fonction	Limite	Portée
Import repris	50 MiB/fichier ; parties 1 MiB ; session 24 h	Plafonds serveur ; contrôle SHA-256 et scan à finalisation
Préparation/OCR	200 pages ; OCR jusqu'à 30 pages ; texte 512 KiB	Texte préparé borné ; file liée à la version
Recherche	200 documents ; 20 rooms ; 30 MiB de texte	Refus des corpus excessifs ; pas de recherche sémantique globale
Comparaison	1 200 lignes ; 1 MiB cumulé	Comparaison exacte de texte dans le périmètre autorisé
Rédaction PDF	30 pages ; 100 régions	Sélection et validation humaines ; original conservé
Clôture ZIP	100 sources ; 50 MiB de sources	Export en clair ; consentement explicite ; manifeste SHA-256
IA assistant	8 documents ; 6 000 caractères/source ; 48 000 cumulés	Extraits sélectionnés ; citations et revue humaine
API	20 clés actives ; 50 rooms/clé ; 1–90 jours	Métadonnées en lecture seule ; quotas 10–100 000/jour
Sessions humaines	8 heures fixes	Révocation serveur ; assurance MFA/passkey contrôlée
Partner	Ticket 60 s ; grant 30 min	Ticket consommable une fois ; scopes limités
Conservation	1–3 650 jours ; rooms CLOSED	Automatisation opt-in ; holds protégés ; sauvegardes séparées
Audit/export	CSV audit 10 000 ; PDF 2 000 événements	Filtres nécessaires ; aucun export silencieusement partiel

Matrice de contrôles et preuves

Les états décrivent ce qui est prouvé à la date de référence. Les preuves détaillées contenant des informations opérationnelles sont fournies dans un cadre de revue approprié, distinct de ce dossier partageable.

ID	Contrôle	État	Preuve	Limite
SEC-01	Isolation tenant et scope des routes	Production — périmètre documenté	Tests de périmètre, memberships, grants, relations composites	Pas d'isolation physique implicite en mode partagé
SEC-02	Mot de passe, MFA, passkeys	Production	Parcours auth/MFA/anti-rejeu/passkey et restauration	SSO/SAML/SCIM à qualifier
SEC-03	Délégation Partner	Production	Preuve live du 06/10 : login, scopes et refus KYC	Grant 30 min ; refus sous politique MFA incompatible
SEC-04	Registre de sessions révocables	Production — qualifié en CI	Test de révocation indépendante et unités assurance	Révocation vérifiée sur fixtures ; maintien des contrôles live
SEC-05	Permissions PDF et filigranes	Production	Prévisualisation protégée et téléchargement refusé en live	Capture physique/écran possible
SEC-06	NDA versionné	Production — qualifié en CI	Signature, preuve immuable, révision et revalidation d'accès	Rooms historiques en mode legacy
SEC-07	AES-256-GCM par objet	Production	10 objets restaurés déchiffrés ; rotation/retour de clés	Métadonnées/volumes non couverts universellement
SEC-08	Chiffrement PII et index aveugles	Production — périmètre documenté	65 valeurs PII dans l'exercice ; contextes d'analyse/confidentialité	Périmètre de champs sélectionnés
SEC-09	Antivirus et conversion isolée	Production	Scan obligatoire, refus EICAR, parcours de restauration	Signatures/format seuls insuffisants
SEC-10	Import chiffré repris	Production — qualifié en CI	Parties, reprise, expiration et finalisation idempotente	50 MiB/fichier ; reprise du même original
SEC-11	Préservation légale	Production — qualifié en CI	Triggers et tests de hold sur document/room/historique	Levée humaine ; motif chiffré
SEC-12	Rédaction brûlée	Production — qualifié en CI	Extraction native + OCR indépendant ; original conservé	Sélection humaine ; nouvelle version non publiée
SEC-13	Audit HMAC et exports	Production — périmètre documenté	Chaîne par tenant ; exports et tests	Pas de WORM externe ni horodatage qualifié

ID	Contrôle	État	Preuve	Limite
SEC-14	Clés API scopes/quota/révocation	Production — qualifié en CI	Scénario API ; stockage uniquement hash ; refus hors scope	Métadonnées seulement
SEC-15	Egress IA approuvé	Production — périmètre documenté	Tests de politique ; citations exactes ; revue humaine	Contrat fournisseur et région à confirmer
SEC-16	Outbox messagerie	Production — qualifié en CI	Baux, idempotence et contrôle des droits dans le code	Acceptation fournisseur ≠ inbox ; pas d'envoi client en test
SEC-17	Conservation et purge physique	Production — qualifié en CI	Hold bloque purge ; fichier effacé ; preuve backupsDeleted=false	NDA/audit/sauvegardes séparés
SEC-18	Demandes de confidentialité	Production — qualifié en CI	Scope, chiffrement, revue et export propre	Pas d'effacement GDPR universel automatisé
SEC-19	Images signées et scans CI	Production	Reçus entreprise.18/20 ; signatures et digests de trois images	Scans au seuil configuré ; pas un pentest indépendant
SEC-20	Restauration chiffrée	Production/exercice	Rapport 07/10 du schéma entreprise.25 ; timer hebdomadaire installé	Perte hôte/DNS/région indépendante à qualifier
SEC-21	Certifications/pentest indépendant	Externe non établi	Aucun certificat ou rapport tiers revendiqué	SOC 2, ISO 27001 et pentest restent à obtenir
SEC-22	Support et astreinte humaine	Contractuel non établi	Collecte et santé techniques uniquement	Couverture 24/7 à convenir

Démonstrations clientes, accès temporaires et guide

Un propriétaire Partner crée un espace de démonstration distinct, pour une durée de 1 à 24 heures, quatre heures par défaut. Cinq démonstrations peuvent être actives simultanément. Le contenu initial est fictif : une room et un PDF synthétiques, un propriétaire et un participant. Aucun dossier client n'est copié.

Les identifiants aléatoires sont affichés une seule fois au créateur ; seuls leurs hashes de mot de passe sont conservés. Le domaine doit passer une vérification HTTPS avant partage. Le guide présente des liens vers les écrans réels, avec étapes, retour, passage, reprise et indication du temps restant.

Une échéance immuable est vérifiée par le serveur. L'accès est refusé après expiration même si le nettoyage périodique est momentanément indisponible. Le nettoyage supprime les appartenances et invitations, révoque grants, sessions et clés API, retire les identifiants des comptes fictifs et désactive le tenant. Les rooms et traces d'audit restent conservées pour la revue opérationnelle : cette procédure est une suppression d'accès, pas un effacement universel des données.

Les appels aux fournisseurs d'IA, les opérations de paiement, d'inscription et d'administration d'identités sont bloqués dans la démonstration. Les destinataires synthétiques ne sont jamais remis au fournisseur de messagerie ; les alertes d'administration/NDA de ces espaces sont également supprimées. Les participants ne disposent pas des droits administratifs du propriétaire et ne peuvent pas consulter une autre démonstration.

Les écrans d'erreur, de service indisponible et de page introuvable utilisent les composants de marque et proposent un retour ou une reprise fonctionnels. Les messages publics n'incorporent pas le détail de l'exception. Les contrôles mobiles couverts ne constituent pas un audit WCAG exhaustif.

Sources techniques : `src/lib/demo-workspace.ts` ; `src/lib/demo-policy.ts` ; `src/proxy.ts` ; `src/components/shared/DemoGuide.tsx` ; `src/app/api/demo/context/route.ts` ; `src/app/error.tsx` ; `src/app/not-found.tsx` ; `src/app/global-error.tsx`

Pilotage institutionnel, cohortes et échéances

Le tableau Deal operations fournit une photographie bornée des rooms du tenant : documents publiés et brouillons, couverture des pièces obligatoires, questions racines ouvertes/en retard/en attente de revue, âge de la plus ancienne question et médiane des délais de réponse enregistrés pendant la période. Les transitions de cycle proviennent des événements effectivement enregistrés ; une histoire antérieure ou des modifications hors workflow ne sont pas reconstituées.

Les cohortes agrègent les groupes de room et les entreprises légales. Seuls les participants humains approuvés disposant actuellement de grants non expirés et non révoqués sont comptés. Une même personne peut appartenir à plusieurs cohortes ; leurs totaux ne doivent pas être additionnés. Les ouvertures, nombres de documents ouverts et durées remontées par le navigateur ne prouvent ni lecture, ni compréhension, ni intention d'achat. Chaque durée est plafonnée à cinq minutes par événement.

Le snapshot PostgreSQL utilise une transaction RepeatableRead et relit les droits avant restitution. Les plafonds sont 50 rooms, 5 000 enregistrements par catégorie, 500 cohortes, 5 000 appartenances et 50 000 événements. Les dépassements sont refusés explicitement. Les filtres de dates UTC et panneaux sont conservés dans l'URL partageable de la vue ; aucune donnée de document n'est stockée comme personnalisation locale.

Les exports CSV/PDF sont réservés aux rôles humains autorisés ; les accès Partner délégués et les rôles support ne peuvent pas exporter ce rapport. L'export est borné à 2 000 lignes et 20 MiB, accompagné des définitions, dates et preuve d'audit durable. La marque utilise le nom configuré du workspace ; le PDF n'incorpore aucune ressource externe.

L'éditeur d'échéances convertit les horaires du fuseau du navigateur en instants ISO explicites, refusant des dates invalides ou inexistantes. Les règles affichent document, état et échéance et peuvent être rechargées pour modification. La recherche du lecteur travaille uniquement sur le PDF déjà autorisé, avec limites de 200 pages, 100 caractères de requête et 500 000 caractères extraits. Les pages scannées/raster peuvent ne pas être recherchables. Seul le numéro de page, lié à utilisateur, document et version, est conservé dans sessionStorage ; ni octets, ni texte, ni titre ne sont mémorisés.

Les modèles de comité contiennent une à trois étapes et un à trois relecteurs distincts par étape. Tous les votes de chaque étape sont nécessaires. Auteur et demandeur sont exclus des relecteurs ; les comptes doivent être humains, approuvés et encore habilités. La décision est liée à la révision exacte du brouillon Q&A ou à la transition de room et à la révision de sa politique. Une édition ou un changement de politique rend la demande obsolète. Le propriétaire peut imposer le comité aux publications Q&A et aux transitions sélectionnées ; les anciens raccourcis sont alors refusés. Une exception requiert une raison chiffrée et un autre propriétaire indépendant. Le comité ne constitue pas un orchestrateur arbitraire de transactions.

Sources techniques : `src/lib/operations-report.ts` ; `src/lib/operations-metrics.ts` ; `src/lib/operations-access.ts` ; `src/app/api/admin/reports/operations/export/route.ts` ; `src/lib/access-dates.ts` ; `src/components/shared/PdfViewer.tsx` ; `src/lib/committee-review.ts` ; `src/app/api/admin/committees/route.ts`

Annexe : réponses au questionnaire acheteur

Ces réponses peuvent être reprises dans une diligence fournisseur. Elles doivent rester accompagnées de la date, de la version et des limites associées.

Question	Réponse	À confirmer
Les fichiers sont-ils chiffrés ?	Oui, objets couverts par AES-256-GCM avec clé de données par objet ; sauvegardes distantes chiffrées.	Vérifier la topologie, les clés et le périmètre de métadonnées.
Le MFA est-il obligatoire ?	Politique configurable par espace ; enrôlement requis avant enforcement.	Attribuer et revoir la politique ; qualifier l'IdP si SSO requis.
Les opérateurs peuvent-ils consulter le KYC ?	La délégation Partner testée est exclue des routes KYC sensibles.	Revoir les comptes humains et les rôles de l'espace.
Pouvez-vous empêcher les captures d'écran ?	Aucune garantie universelle ; contrôle d'accès et filigranes disponibles.	DRM/IRM externe et conditions d'usage à définir si nécessaires.
Disposez-vous de SOC 2/ISO 27001 ?	Aucune certification obtenue n'est déclarée dans ce dossier.	Définir audit externe, périmètre et preuve requise.
Quel RPO/RTO garantissez-vous ?	Aucun engagement établi ici ; runbook cible 24 h/4 h, exercice de restauration disponible.	Qualifier perte d'hôte, clés, DNS et contrat.
Où sont les données ?	Dépend du déploiement, de ses sauvegardes et sous-traitants.	Annexe de régions et flux à approuver avant commande.
Les données sont-elles envoyées à une IA ?	Uniquement sur chemin activé/approuvé ; catégories confidentielles exigent approbation.	Confirmer fournisseur, DPA, région et règles de traitement.
Les suppressions retirent-elles les sauvegardes ?	Non ; la purge documentée n'efface pas les sauvegardes.	Accorder politique de conservation et procédure de fin de contrat.
Le service assure-t-il une réponse humaine 24/7 ?	Non revendiqué sans équipe/contrat démontrés.	Définir horaires, canaux et objectifs de réponse.
L'API donne-t-elle accès aux fichiers ?	Le nouveau périmètre documenté est la lecture de métadonnées autorisées.	Définir les intégrations supplémentaires nécessaires.
Les NDA sont-ils des signatures qualifiées ?	La preuve applicative n'est pas déclarée qualifiée.	Faire valider les exigences juridiques et le fournisseur éventuel.

Références de preuve

Livraison entreprise.18 : 6 octobre 2026, 13:39 UTC ; signatures des trois images vérifiées, migrations appliquées, contrôles de connexion sur ordinateur/mobile réussis. Le reçu entreprise.20 confirme la livraison des démonstrations et du pilotage avec le correctif Sharp. Les preuves CI couvrent les refus entre tenants, les droits de rapport, les cohortes, les fuseaux horaires, les téléchargements et la reprise liée à la version. Le lot VDR a passé une campagne CI complète de 60 scénarios et 326 tests unitaires ; le lot démo a passé 343 tests unitaires et son scénario d'expiration. Semgrep strict et scans d'images sont requis avant livraison. L'exercice de restauration du 6 octobre à 06:31 UTC portait sur la sauvegarde antérieure aux migrations complémentaires. L'exercice courant du 7 octobre est postérieur à entreprise.25 et utilise son image exacte : ses résultats qualifient le schéma livré dans une restauration isolée sur l'hôte actuel.

Le fichier source JSON contient la provenance et l'empreinte SHA-256 des fichiers examinés dans la version signée, ainsi que les résultats non sensibles de la restauration courante. Les matrices CSV permettent la reprise des contrôles et réponses dans une revue acheteur. Les rapports opérationnels détaillés peuvent être fournis sous un cadre de confidentialité approprié.

Contact commercial et technique : demande de dossier sur la page Sécurité de [hiveroom.app](#) ou échange avec l'équipe AVA Hive.