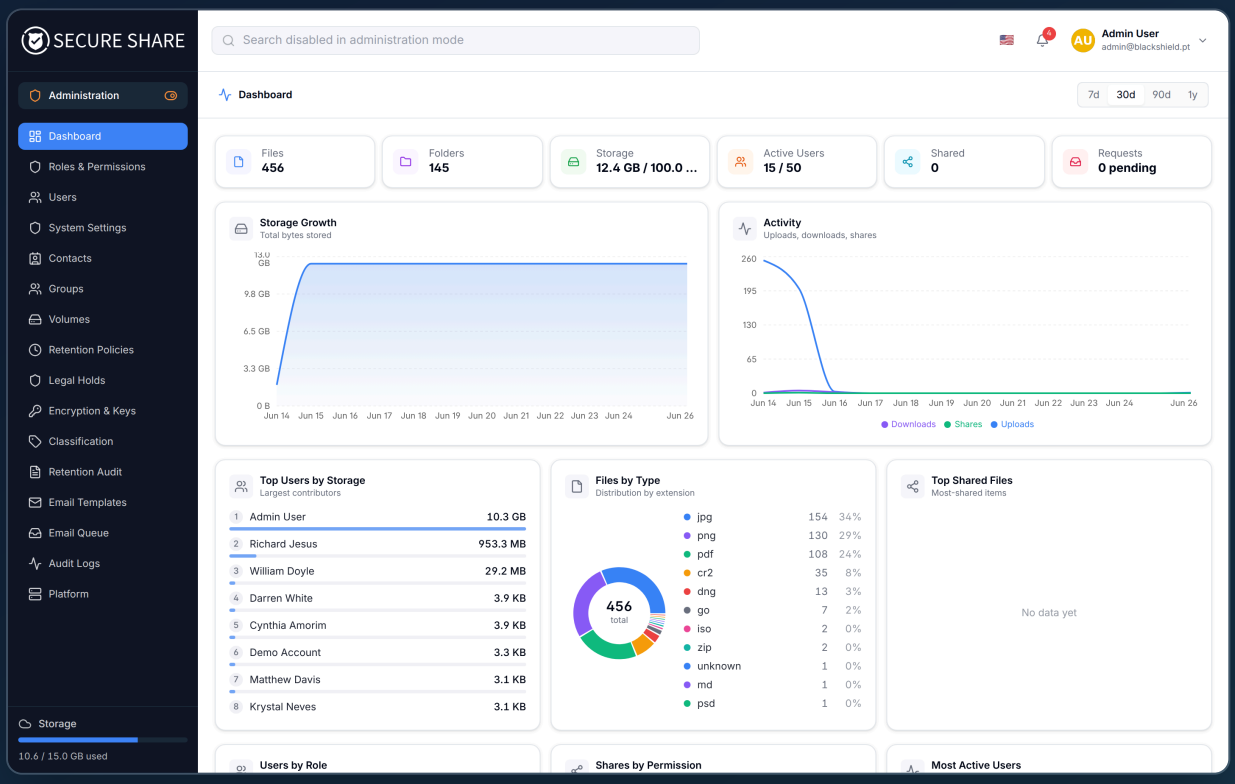
BLACKSHIELD

SECURE SHARE

The Enterprise Platform for Encrypted File Sharing, Storage, and Compliance



A TECHNICAL WHITEPAPER

June 2026

Contents

1 Executive Summary

Organizations move sensitive data every day — contracts, medical records, financial statements, intellectual property, regulated case files. The tools most teams use to share those files were built for convenience, not control. Once a file leaves your hands, you rarely know who opened it, when it expires, or whether it can ever be recovered, revoked, or proven untouched.

SecureShare is an enterprise-grade, multi-tenant platform for **encrypted file storage, sharing, and compliance**. It combines strong cryptography, granular access control, and a complete compliance toolkit — retention policies, legal hold, write-once immutability, and tamper-evident audit trails — in a single, deployable platform.

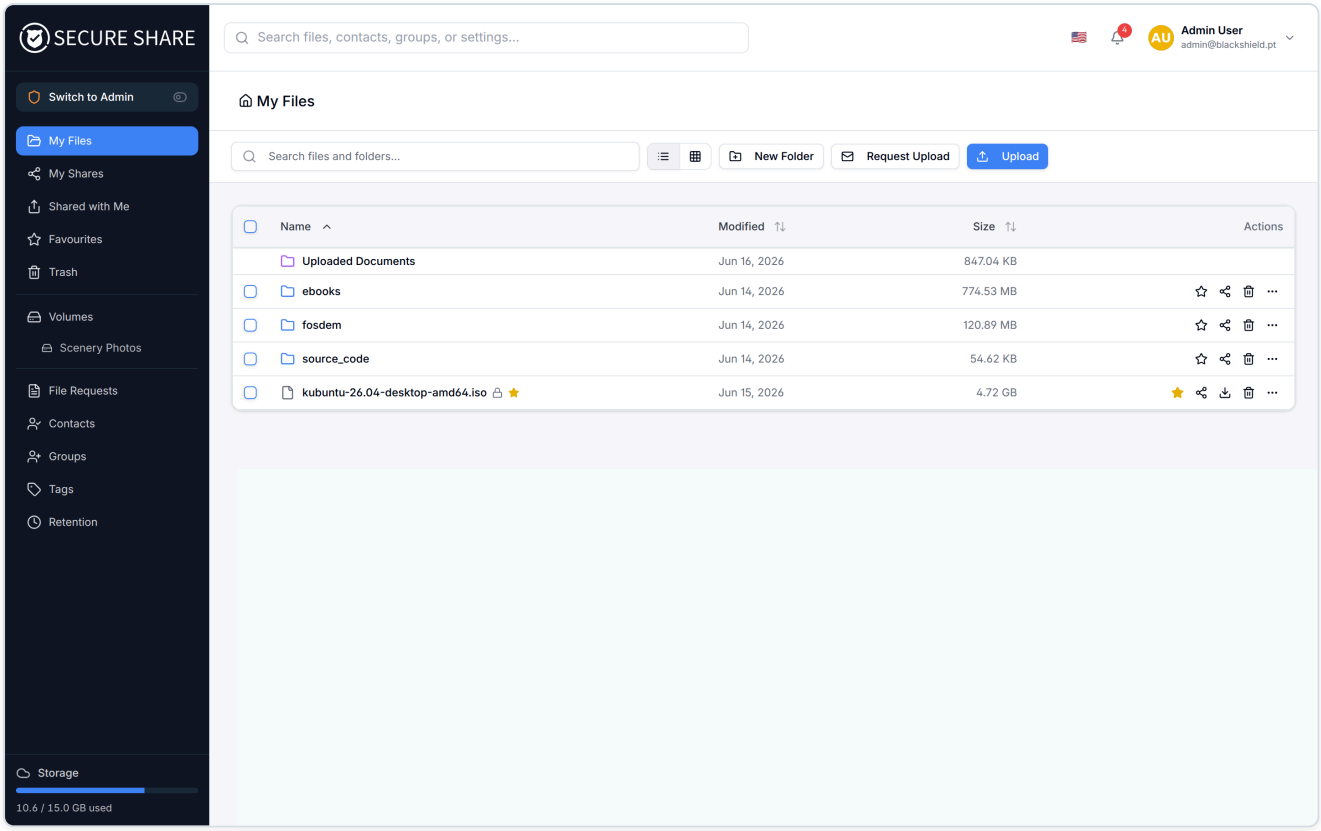
SecureShare is built around three principles:

> **Encryption by default.** Every file is protected with modern authenticated encryption. Organizations can choose transparent server-side encryption, or password-protected client-side encryption — zero-knowledge, where even the platform operator cannot read the data.

> **Control that survives the share.** Expiring links, download limits, password protection, granular permissions, and instant revocation mean that sharing a file never means losing control of it.

> **Accountable governance.** Retention, legal hold, and a tamper-evident audit log help compliance and legal teams show what happened — for GDPR, NIS2, DORA, and internal governance.

© BlackShield



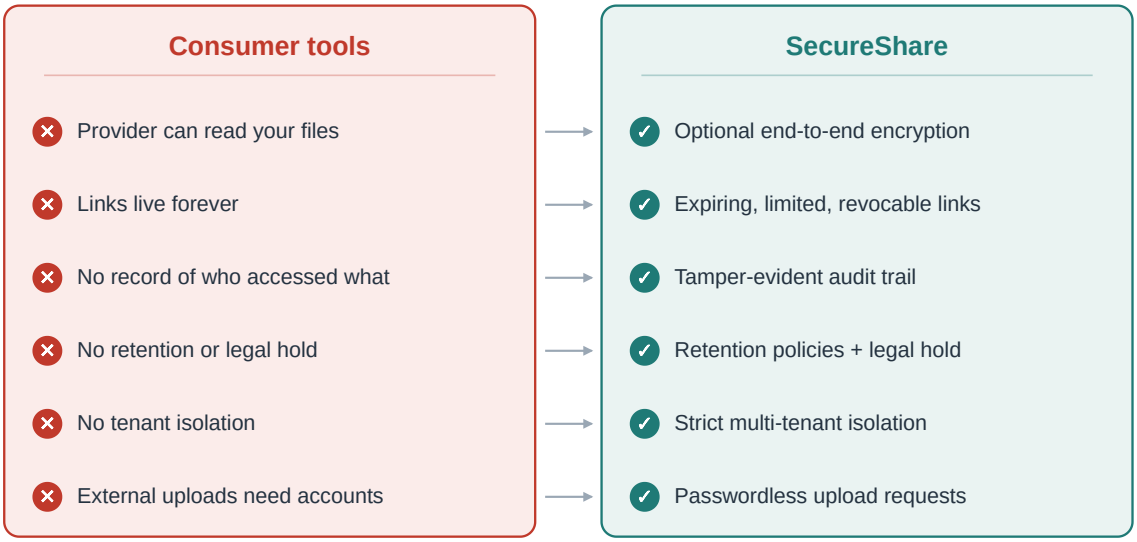
Main dashboard — file overview, storage usage, recent activity widgets

2 The Problem: Sharing Files Without Losing Control

Most file-sharing happens through tools that optimize for speed: consumer cloud drives, email attachments, chat apps. Each of these creates risk that scales with the sensitivity of the data:

Risk	Consumer tools	SecureShare
Data readable by the provider	Yes, in most cases	Optional end-to-end encryption — provider can't read it
Links live forever	Common	Expiration, download limits, instant revocation
No record of who accessed what	Typical	Full, tamper-evident audit trail
No retention or legal hold	Absent	Built-in retention policies + legal hold
No tenant isolation	N/A	Strict multi-tenant data separation
External uploads require accounts	Usually	Passwordless secure upload requests

Regulated industries — healthcare, finance, legal, government — cannot accept these trade-offs. They need to share data **and** retain control, visibility, and provability. SecureShare is built for exactly that intersection.



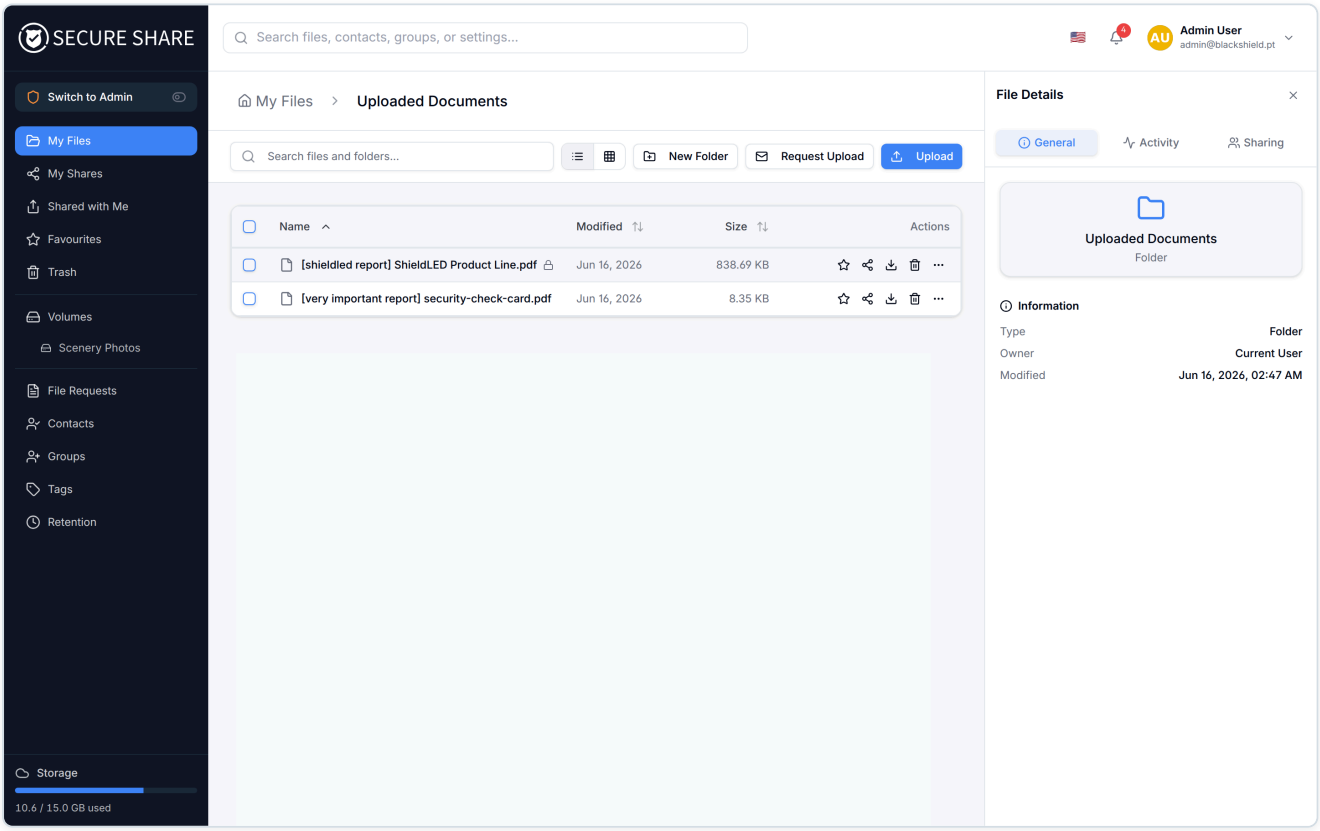
© BlackShield

3 Platform Overview

SecureShare is delivered as a unified platform spanning storage, sharing, identity, compliance, and administration.

Core Capabilities at a Glance

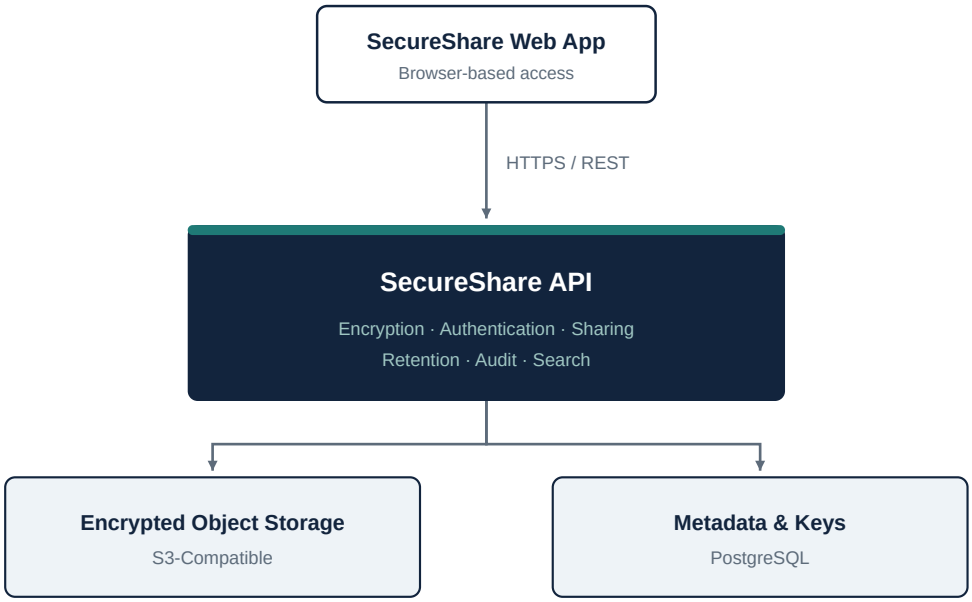
- **Encrypted storage** with pluggable backends (S3-compatible or local filesystem)
- **Two encryption trust models**: transparent server-side, and password-protected client-side (zero-knowledge)
- **Hierarchical key management** with per-tenant key rotation
- **Flexible sharing**: internal permission-based sharing and external public links
- **Secure upload requests** that let external parties send you files without an account
- **Multi-factor authentication** and federated identity (OIDC, LDAP)
- **Role-based access control** with granular permissions
- **Retention, legal hold, and WORM immutability** for compliance
- **Tamper-evident audit logging** with SIEM event forwarding
- **Full-text search** across your files
- **Productivity tools**: volumes, folders, tags, favorites, trash with restore, notifications, and contacts
- **Multi-tenant** architecture with strict data isolation



File browser — folders, files, encryption badges, sharing indicators

How It Fits Together

SecureShare follows a clean separation of concerns: a browser-based web app talks to the SecureShare API over HTTPS/REST, and the API handles all encryption, authentication, sharing, retention, audit, and search. Encrypted file contents are written to S3-compatible object storage, while metadata and wrapped keys live in PostgreSQL — so ciphertext and key material are never co-located in the same store.



© BlackShield

4 Encryption Architecture

Encryption is the foundation of SecureShare. The platform uses modern, authenticated cryptography throughout, and gives organizations a choice of trust model.

Modern Authenticated Encryption

Files are encrypted using **XChaCha20-Poly1305**, a state-of-the-art authenticated cipher with a 24-byte nonce and built-in integrity protection. Every encrypted block carries an authentication tag, so tampering is detected automatically — a modified ciphertext will never decrypt to plausible-looking data. Block ordering is cryptographically bound, preventing reordering or splicing attacks.

Where passwords protect a file, keys are derived using **Argon2id**, the modern, memory-hard password-hashing function recommended for resisting brute-force and GPU-accelerated attacks.

Two Trust Models

SecureShare lets each organization — and each file — match the encryption model to the sensitivity of the data.

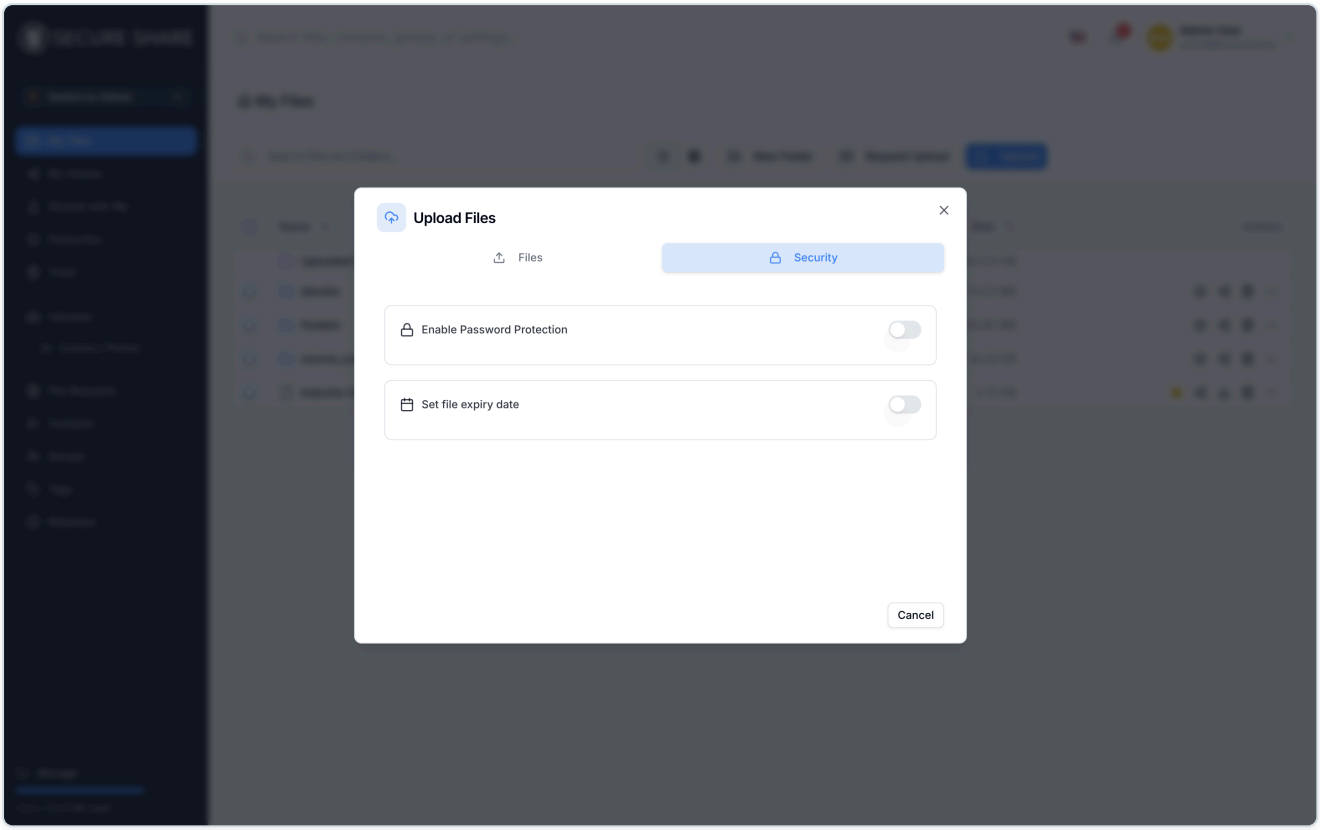
1. Transparent Server-Side Encryption

Files are encrypted automatically at rest. Keys are managed by the platform under a per-tenant key hierarchy. Users get a frictionless experience; administrators get strong at-rest protection with no behavior change. Ideal for general business data.

2. Password-Protected, Client-Side Encryption

When a password is set, the file is encrypted **in the browser** before it ever reaches the server, using the SecureShare crypto library. The recipient must supply the password to decrypt, and the platform stores only ciphertext — it never sees the password or the plaintext. This delivers true **zero-knowledge** confidentiality: even a fully compromised server cannot reveal the contents, making it ideal for your most sensitive material. For organizations that cannot risk permanent data loss, an optional administrative recovery path is available (see below).

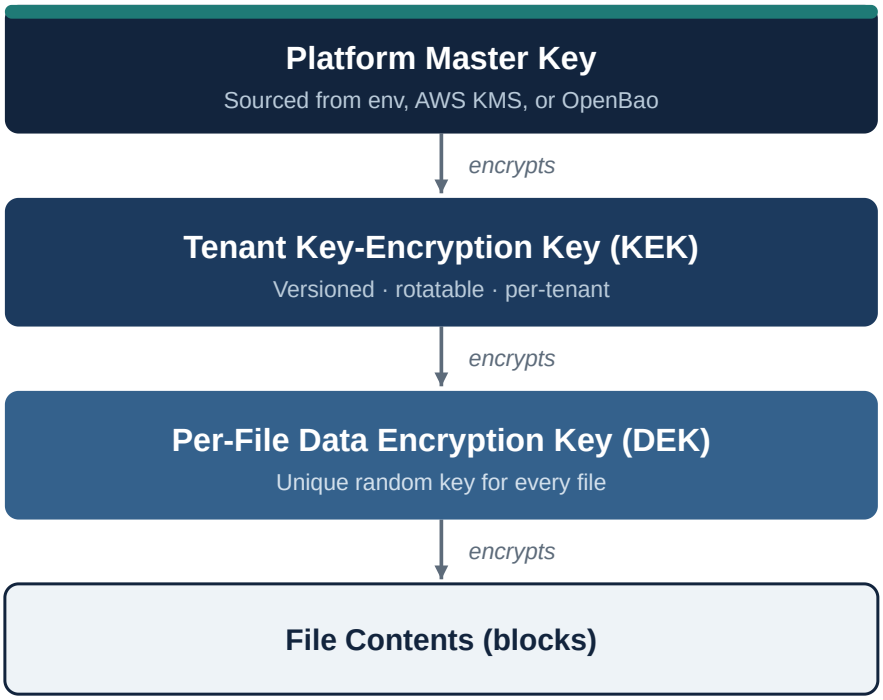
© BlackShield



Upload dialog (Security tab) showing the password-protection and file-expiry toggles

Hierarchical Key Management

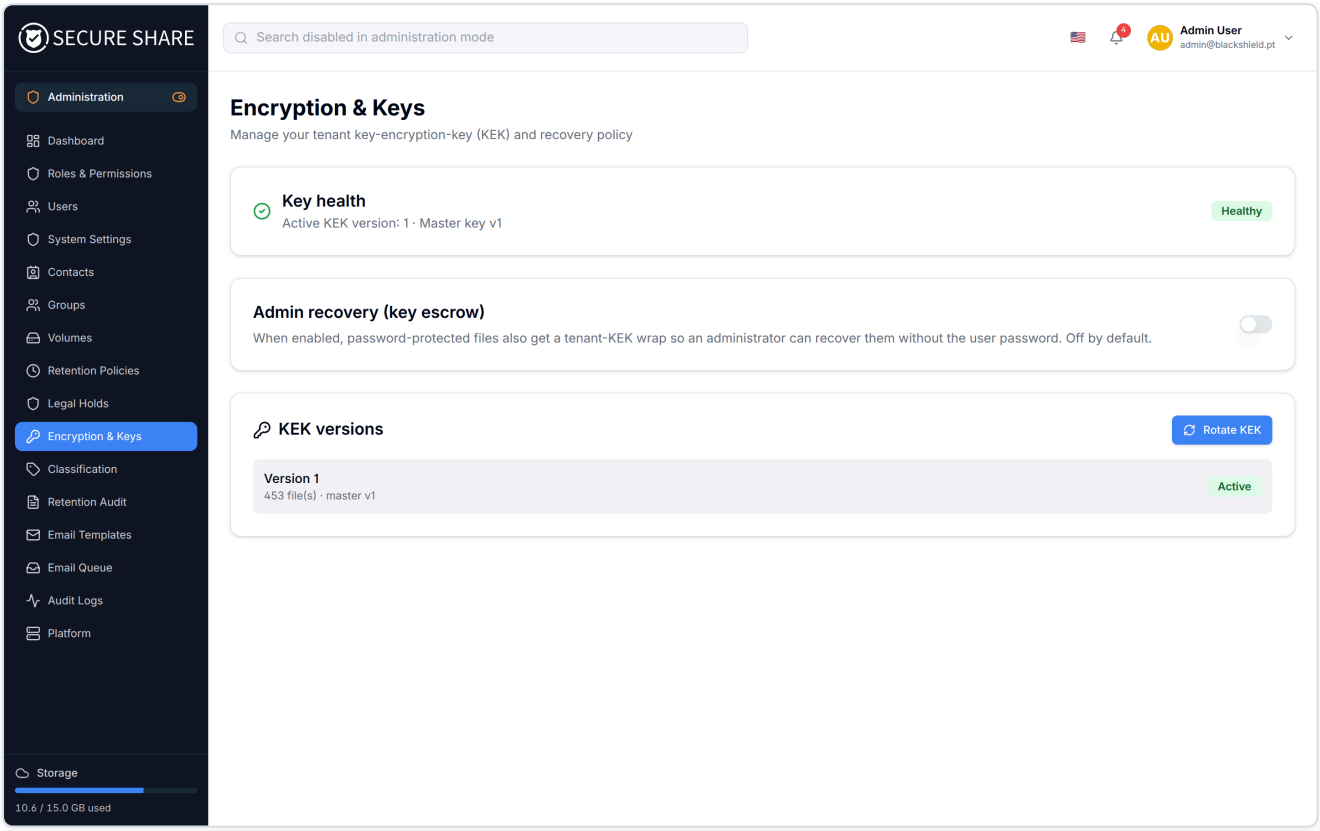
SecureShare protects keys with keys, in a layered hierarchy that limits the blast radius of any single exposure and enables rotation without re-encrypting data wholesale.



© BlackShield

- **Master Key** — the root of trust, loaded at startup from an environment secret, **AWS KMS**, or **OpenBao** (HashiCorp Vault-compatible). It never touches disk in plaintext and is never logged.
- **Tenant KEK** — each tenant has its own versioned Key-Encryption Key, stored encrypted under the master key. Keys can be **rotated** on a schedule; rotation re-wraps file keys in the background without downtime.
- **Per-File DEK** — every file gets a unique, randomly generated Data Encryption Key. Compromise of one file's key never affects another.

This design means key rotation is fast (re-wrap keys, not re-encrypt terabytes), tenant isolation is cryptographic, and integration with enterprise key-management infrastructure (KMS / Vault) is native.



Admin key management / KEK rotation panel

Administrative Recovery (Optional)

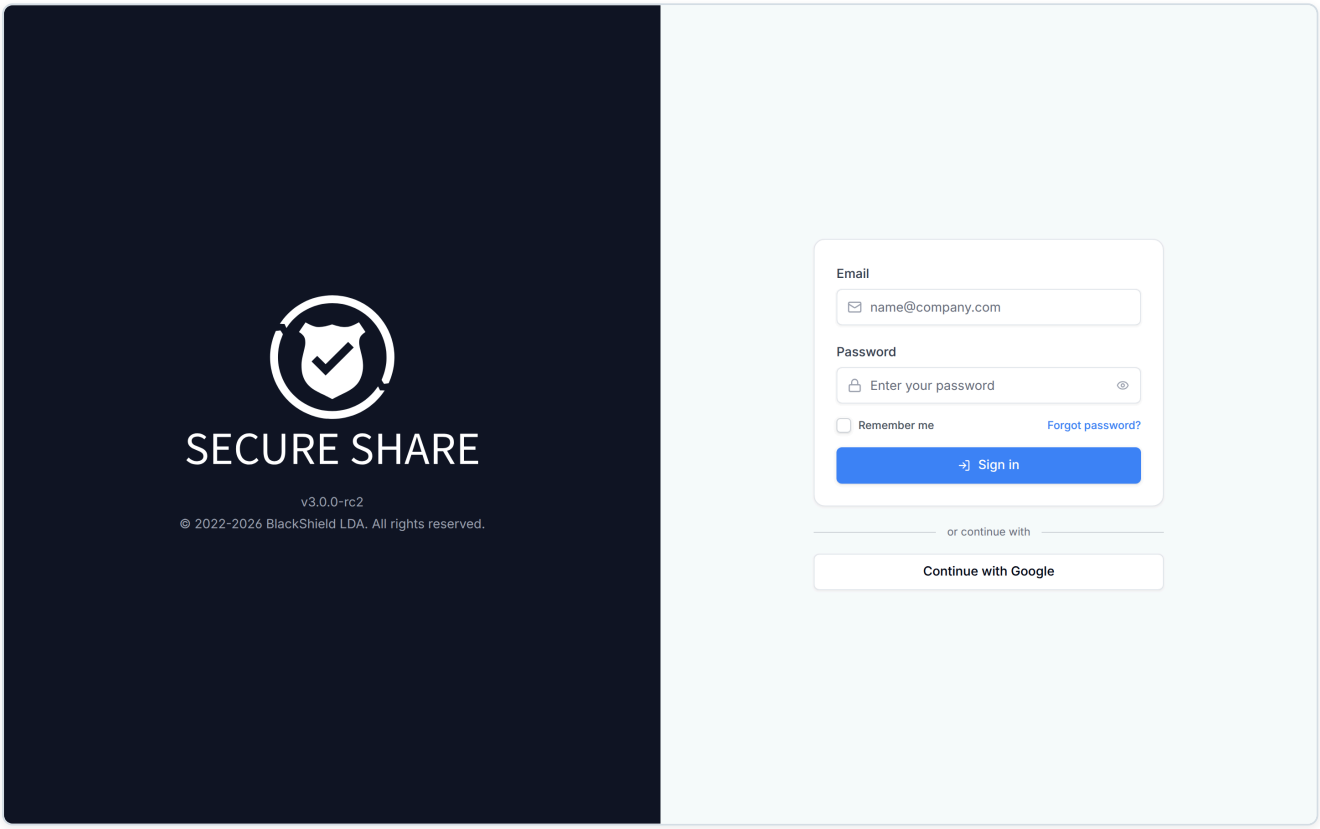
For organizations that cannot risk permanent data loss when an employee forgets a password or leaves, SecureShare offers an **optional administrative recovery** capability on password-protected files. When enabled per tenant, files carry a second, KEK-protected key wrap so authorized administrators can recover data through governed, audited channels. Organizations that require strict zero-knowledge can leave it disabled — the choice is yours.

5 Identity, Authentication & Access Control

SecureShare meets enterprises where their identity infrastructure already lives.

Authentication Options

- **Local accounts** with strong password hashing
- **LDAP / Active Directory** — bind and search integration with TLS
- **OIDC federation** — single sign-on with Google, Microsoft Entra, Okta, Keycloak, GitLab, and any standards-compliant provider, using PKCE and state protection
- **Multi-factor authentication (MFA)** — TOTP-based (compatible with Google Authenticator, Authy, 1Password, etc.) with recovery codes



Login screen with Google SSO

Session Security

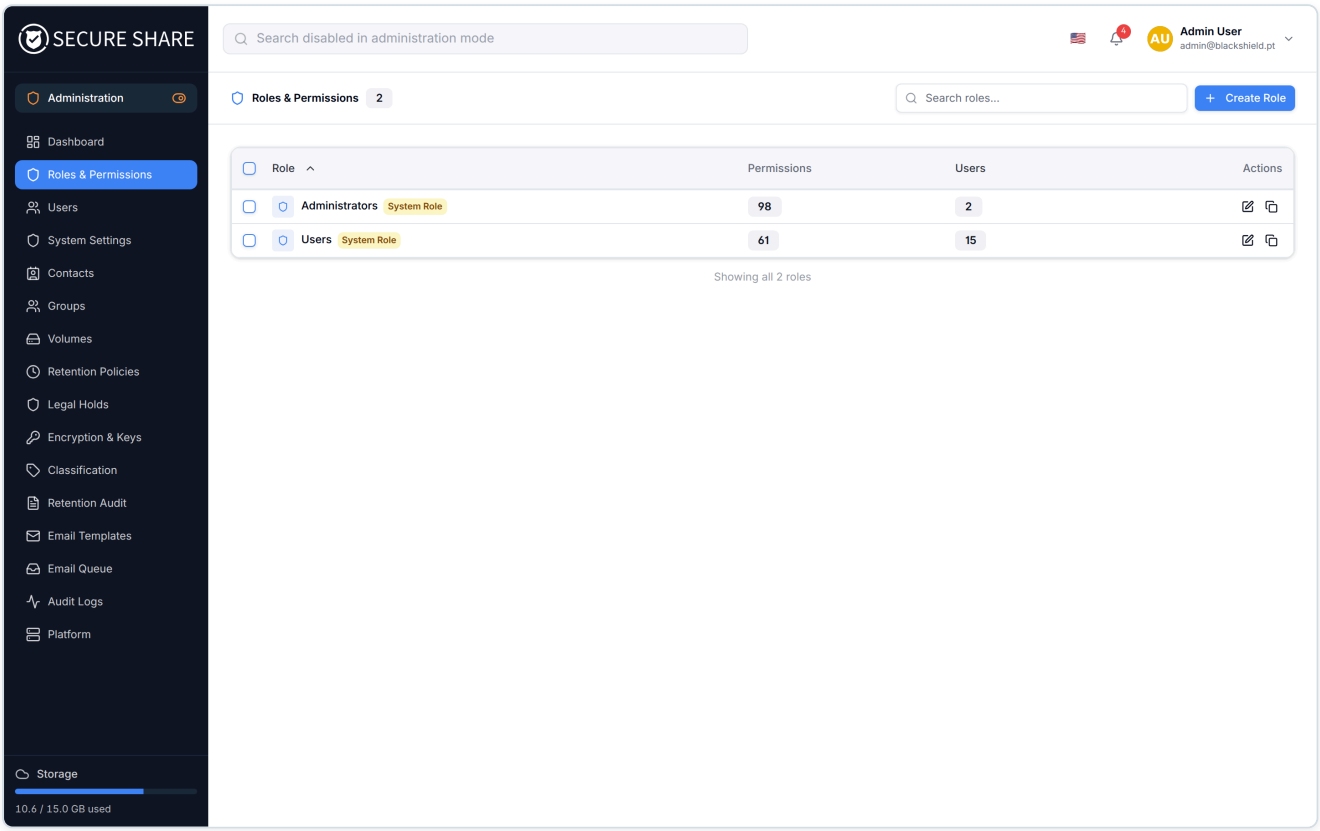
Sessions are protected with encrypted, Redis-backed storage and short-lived access tokens (RS256-signed JWTs) paired with rotating refresh tokens. SecureShare adds:

- **Session fingerprinting** — detects and flags session hijacking by binding sessions to network and client characteristics
- **New-device login alerts** — users and admins are notified by email and in-app when a login occurs from an unfamiliar device
- **Brute-force protection** — adaptive rate limiting per user and per IP address

- **Instant revocation** — sessions and tokens can be revoked immediately on logout or by an administrator

Role-Based Access Control

Access is governed by a flexible RBAC model. Administrators define roles, assign granular permissions (administration, user management, file operations, retention, legal hold, and more), and link them to users. Every file and folder additionally supports its own **access control list**, with permissions that inherit down folder hierarchies.



Roles & permissions admin screen

6 Secure File Sharing

Sharing is where most platforms quietly give up control. SecureShare keeps it.

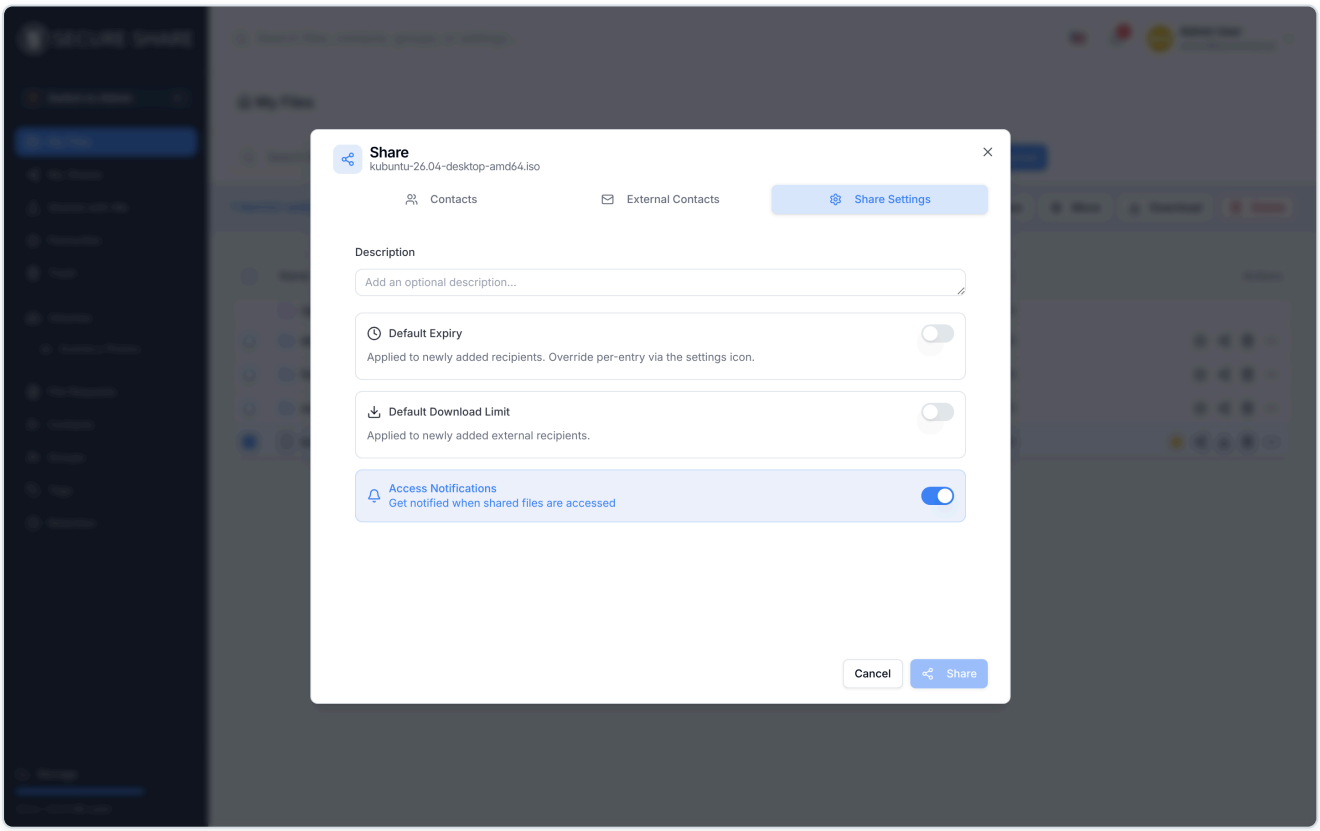
Internal Sharing

Share files and folders with other members of your organization using granular permissions — read, write, delete, manage, view-content — that inherit through folder structures. Every share is access-controlled and recorded.

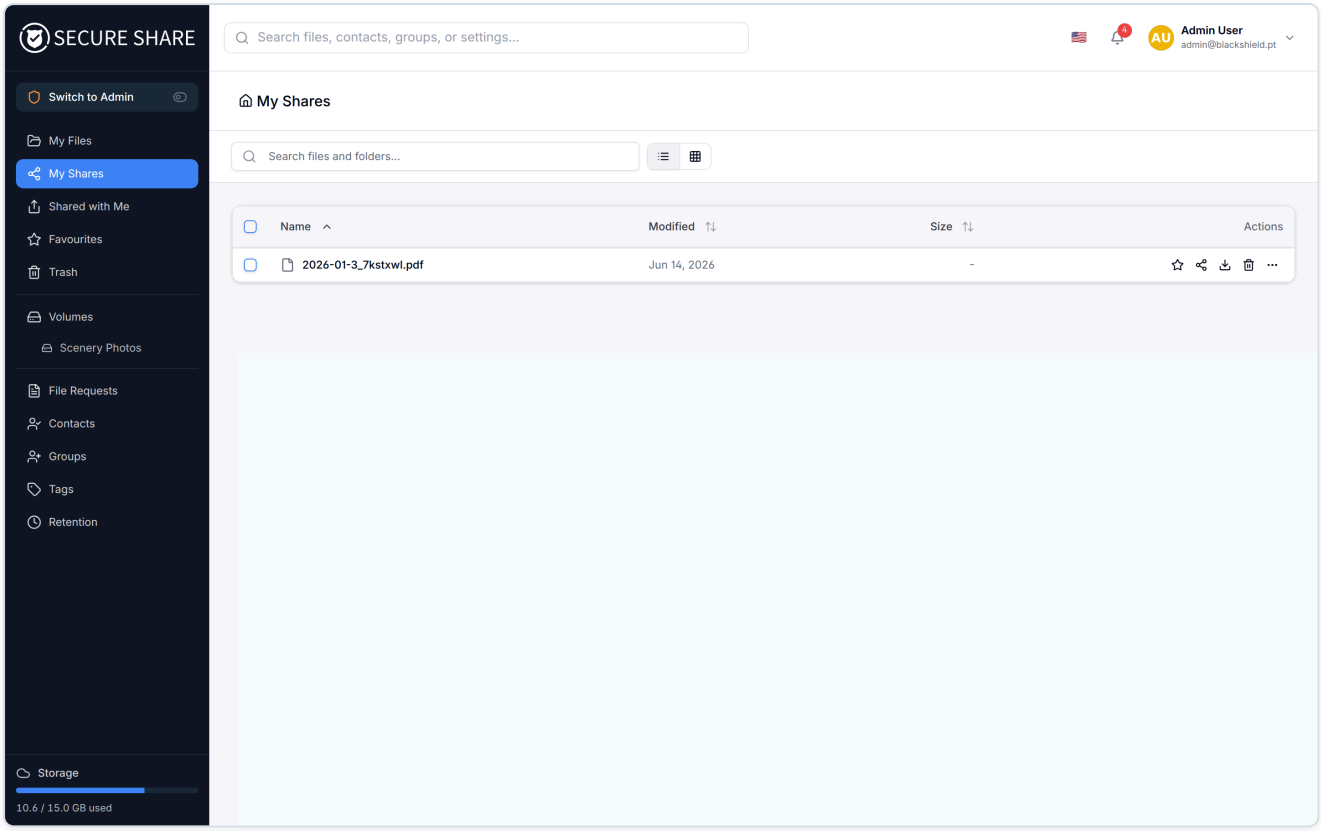
Public Share Links

Share with anyone, anywhere, while keeping control:

- **Expiration dates** — links automatically stop working
- **Download limits** — cap the number of times a file can be retrieved
- **Password protection** — add a password independent of the file's encryption
- **Custom messages** — give recipients context
- **Instant revocation** — kill a link the moment you need to
- **Access tracking** — see who downloaded what, when, and from where



Create share link dialog — expiration, password, download limit controls



Share access log — list of accesses with timestamps and IPs

Verify Without Exposing

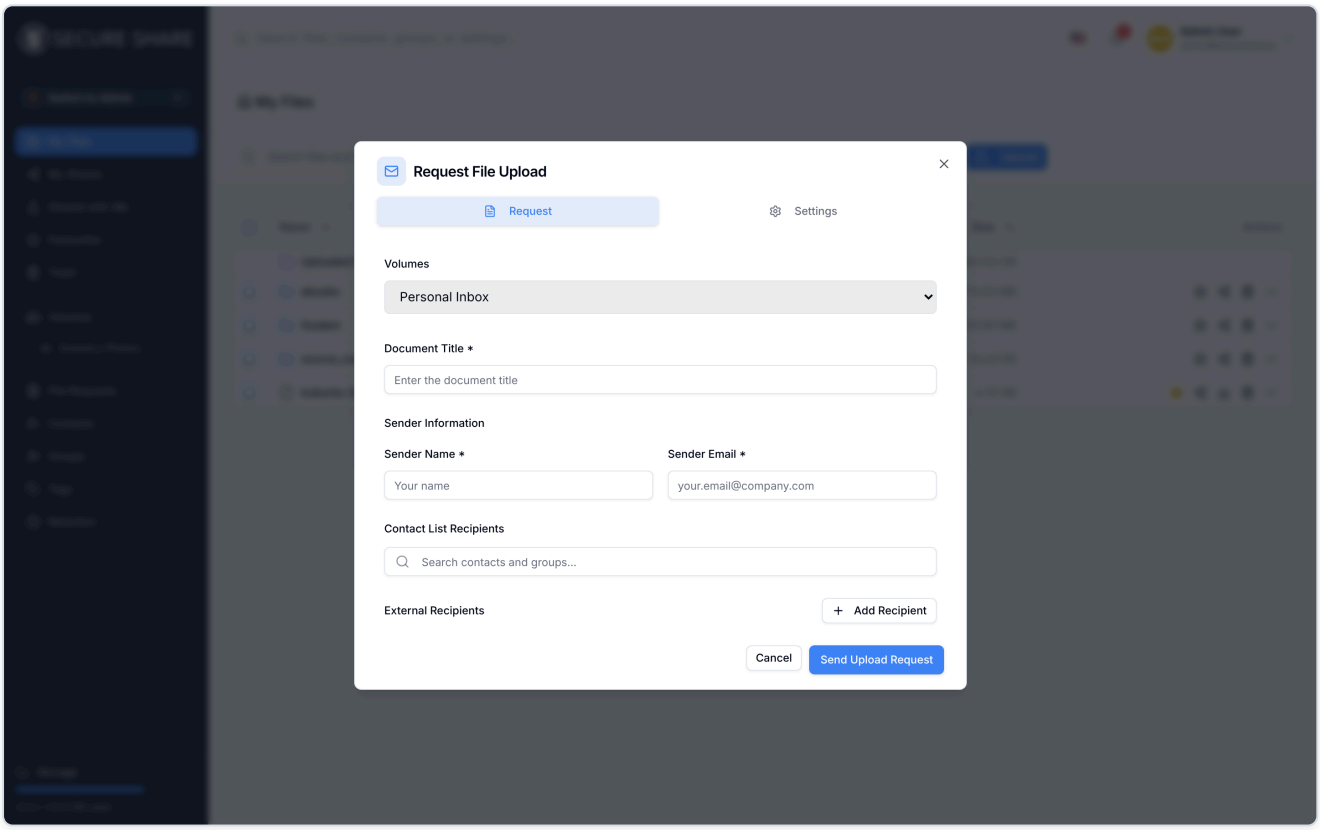
SecureShare can confirm a recipient holds the correct password **before** any decryption occurs, so failed attempts never expose ciphertext or consume protected data.

7 Collecting Files: Secure Upload Requests

Sometimes the file needs to come *to* you — from a client, a patient, a counterparty who doesn't have an account.

SecureShare's **secure upload requests** (the Inbox) let you generate a request link that an external party can use to upload files directly into your encrypted storage — **no account required**. Uploads land encrypted, routed to the folder you choose, with full audit recording.

This replaces the insecure habit of emailing sensitive documents back and forth, and it works for any "please send me your files securely" workflow: onboarding documents, signed contracts, medical intake, financial disclosures.



Upload request creation + the external uploader's view

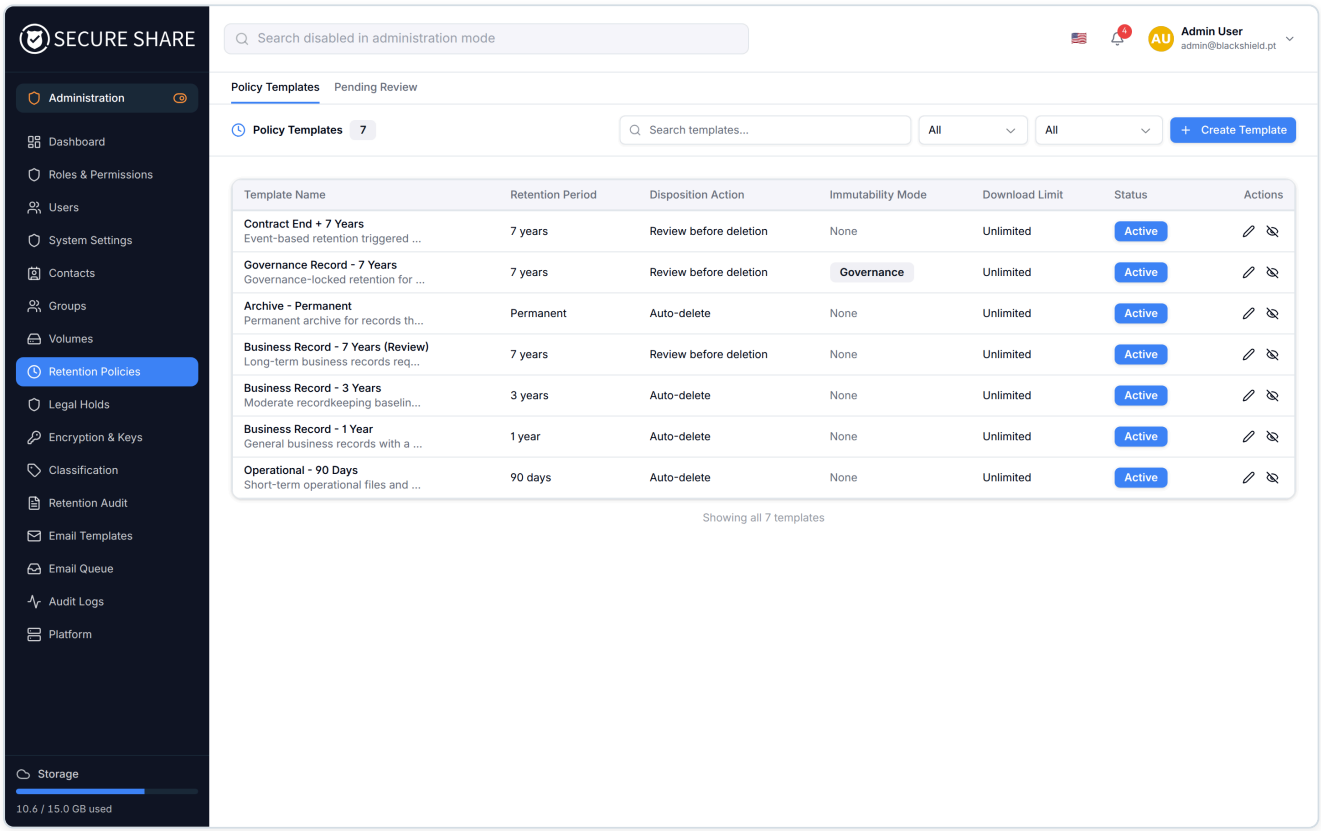
8 Compliance: Retention, Legal Hold & Immutability

SecureShare includes a built-in compliance toolkit — retention, immutability, legal hold, and tamper-evident audit — to support your governance and legal workflows.

> **Early access:** Retention policies, legal hold, and WORM immutability are currently offered as an early-access preview and under active development. Their behavior and configuration may change before general availability; validate them against your own requirements before relying on them for production record-keeping. (Tamper-evident audit logging is generally available.)

Retention Policies

Define **retention policies** that specify how long files are kept and what happens when that period ends. Policies can be applied automatically through **classification rules** — for example, by file type or tag — so the right rules apply without manual effort. Disposition can be time-based or triggered by business events, and end-of-life actions can require human **review and approval** before anything is deleted.



Retention policy configuration screen

Write-Once Immutability (WORM)

For records that must not change, SecureShare offers immutability modes:

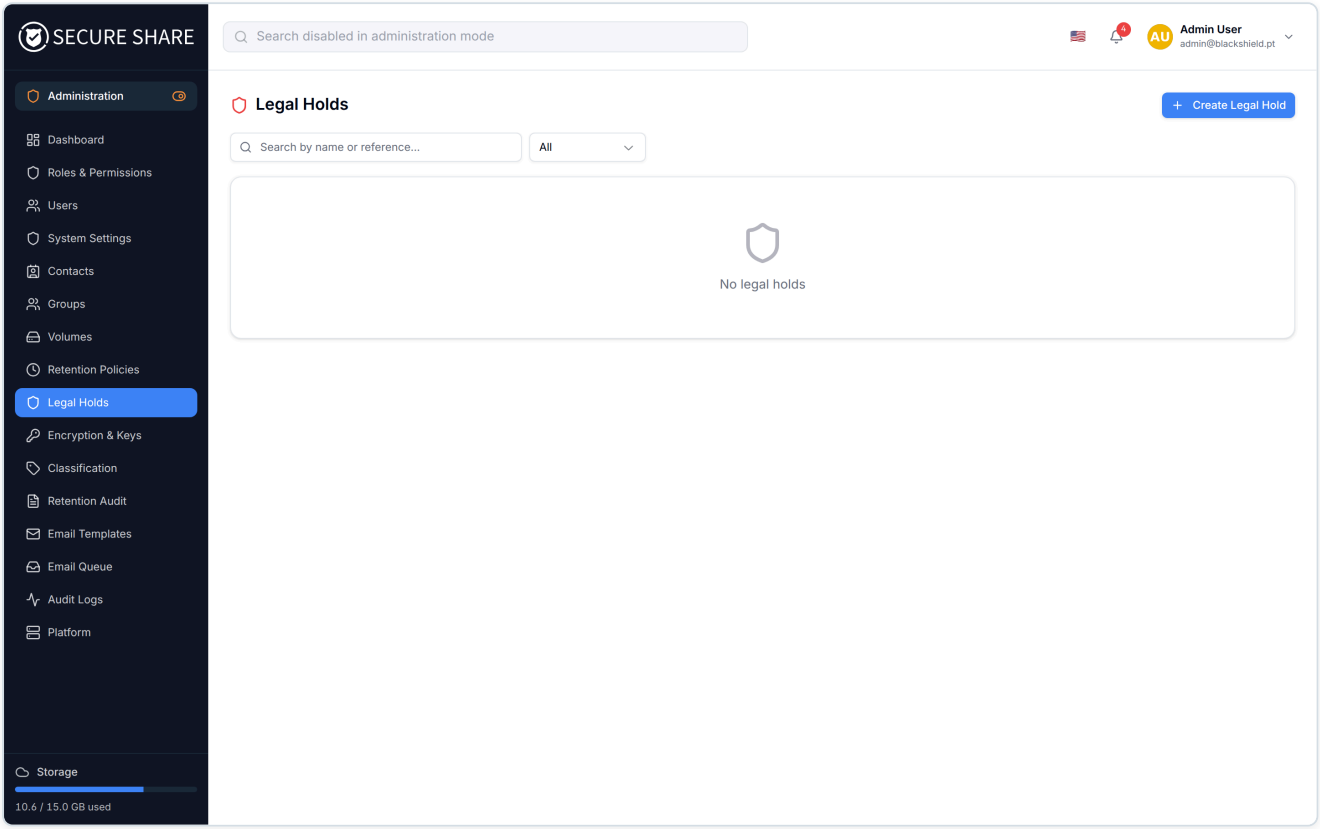
- **Governance mode** — protected against accidental modification, overridable by authorized administrators

- **Compliance mode** — enforced platform-wide; no user or administrator can alter or delete the record through SecureShare before its retention period expires. For end-to-end immutability guarantees, pair it with storage-level object lock (e.g., Amazon S3 Object Lock) on the underlying bucket.

This supports regulatory requirements for long-term, unalterable record-keeping — for example, financial-sector retention mandates under regimes such as DORA.

Legal Hold

When litigation or investigation requires it, place a **legal hold** on files or folders. Held data is frozen — the retention clock stops, deletion is blocked, and disposition is suspended — until the hold is lifted. Every action is recorded with reason and approver.



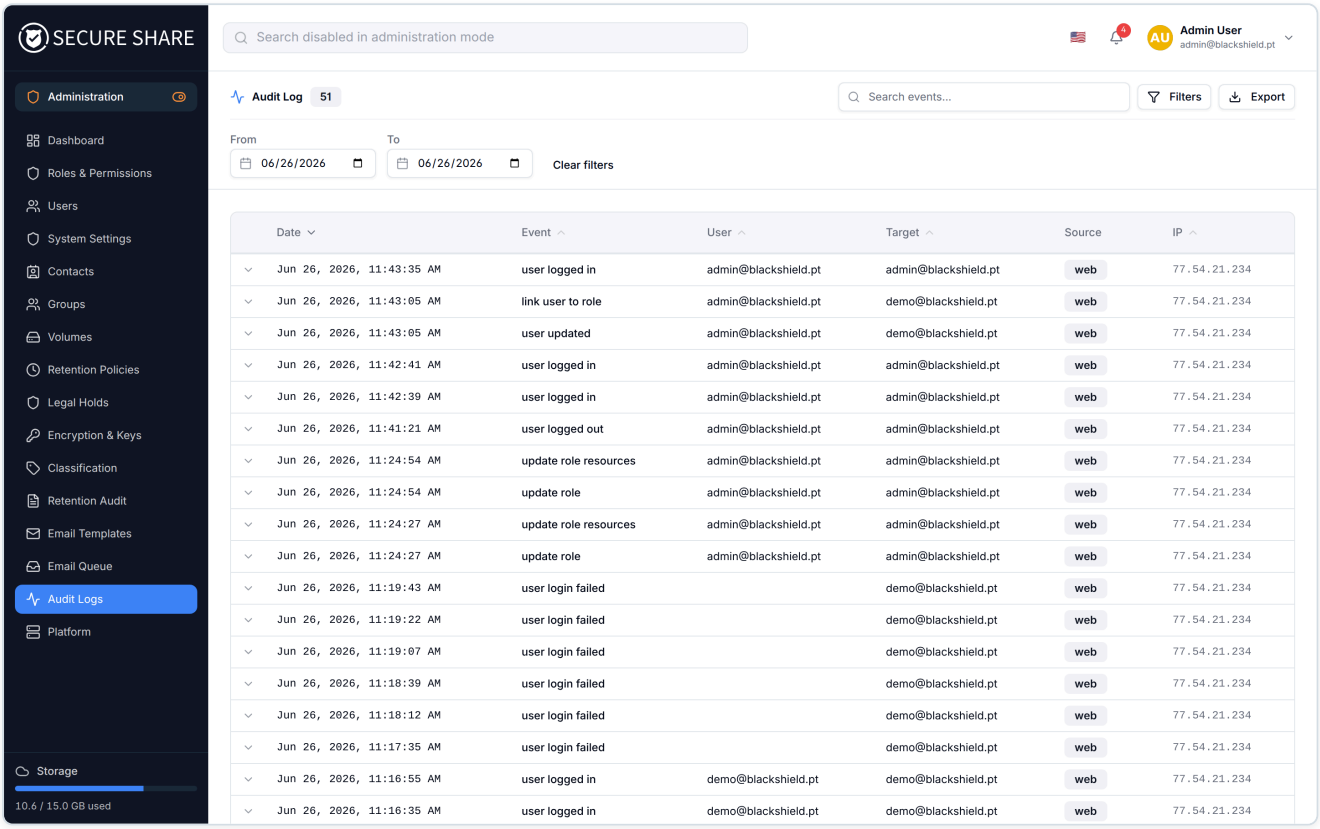
Legal hold management view

9 Audit, Visibility & SIEM Forwarding

If you can't prove it, it didn't happen. SecureShare records the events that matter and makes them tamper-evident.

Comprehensive Audit Trail

Every security-relevant action is logged: logins and logouts, user and role changes, file and folder operations, every share and download, retention and legal-hold transitions, key lifecycle events, and administrative recovery. Each entry captures who, what, when, where (IP address), the outcome, and contextual detail.



Audit log viewer — filterable, paginated event list

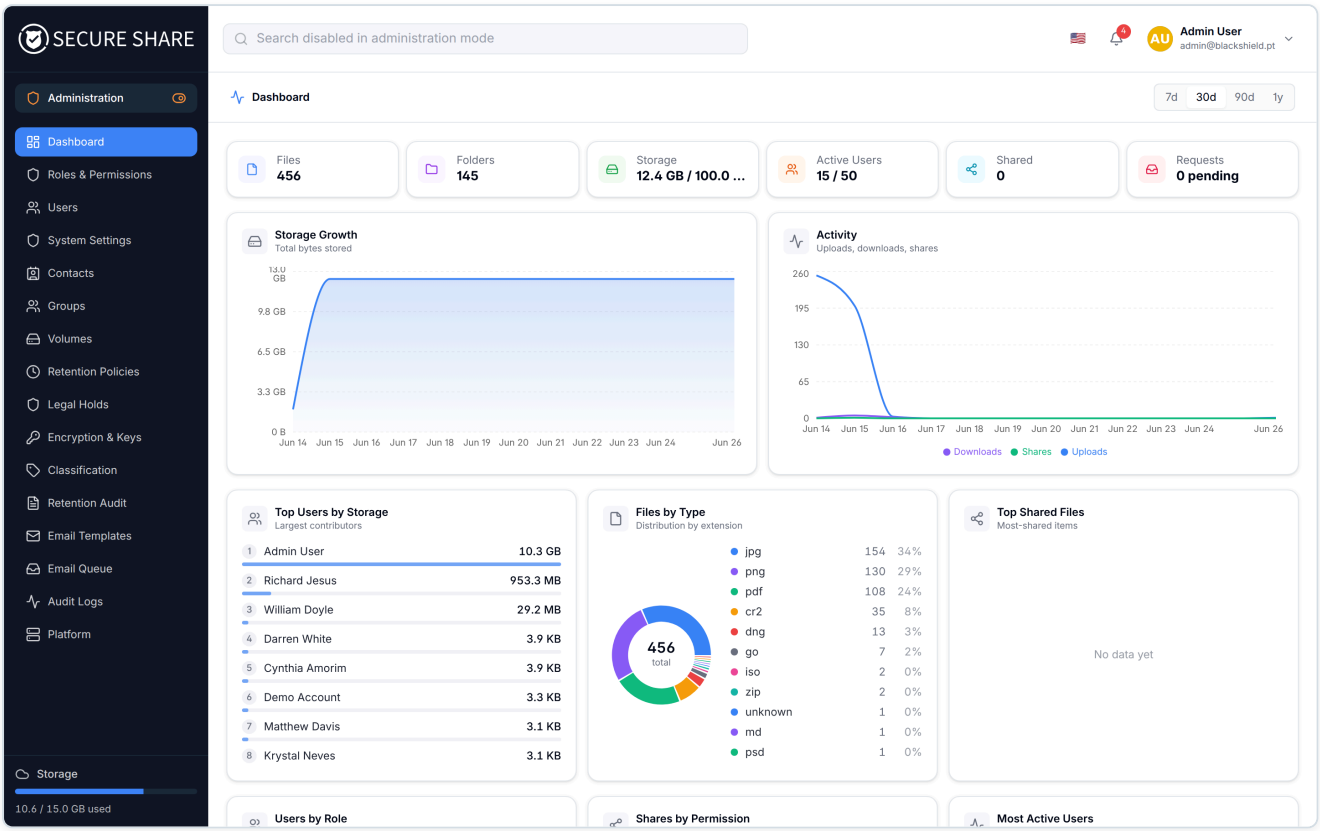
Tamper-Evident Integrity

When enabled, audit records are protected with cryptographic integrity checkpoints — periodic HMAC-based hashes computed over each window of events — so later tampering with stored history can be detected. It makes your audit trail not just complete, but independently **verifiable**.

Enterprise Visibility

- **Audit event webhooks** — forward audit events to your SIEM or security operations platform over HTTP, with event-type filtering
- **Analytics warehouse** — events stream to a high-performance analytics store for reporting and long-term retention

- **Query & extract** — pull audit history from the analytics store for reporting, external systems, and regulators
- **Configurable retention** — keep audit history for as long as regulations require



Admin analytics / statistics dashboard

10 Multi-Tenancy & Administration

SecureShare is built multi-tenant from the ground up, making it equally suitable for a single enterprise with multiple business units, a managed service provider, or a SaaS offering.

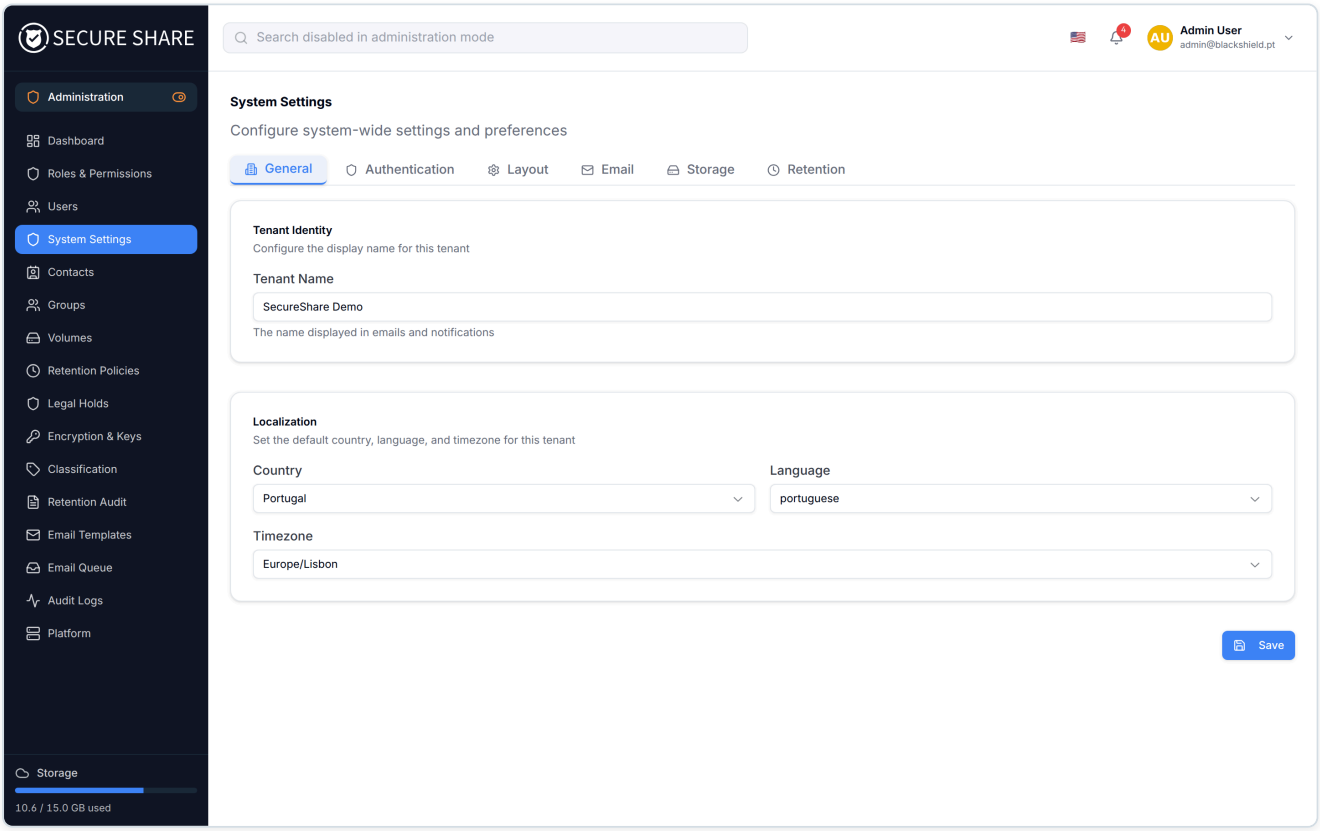
Strict Tenant Isolation

Every tenant's data, keys, users, and configuration are isolated. Tenants are resolved by domain, each has its own cryptographic key hierarchy, and data access is filtered by tenant at every layer. One tenant can never see another's data.

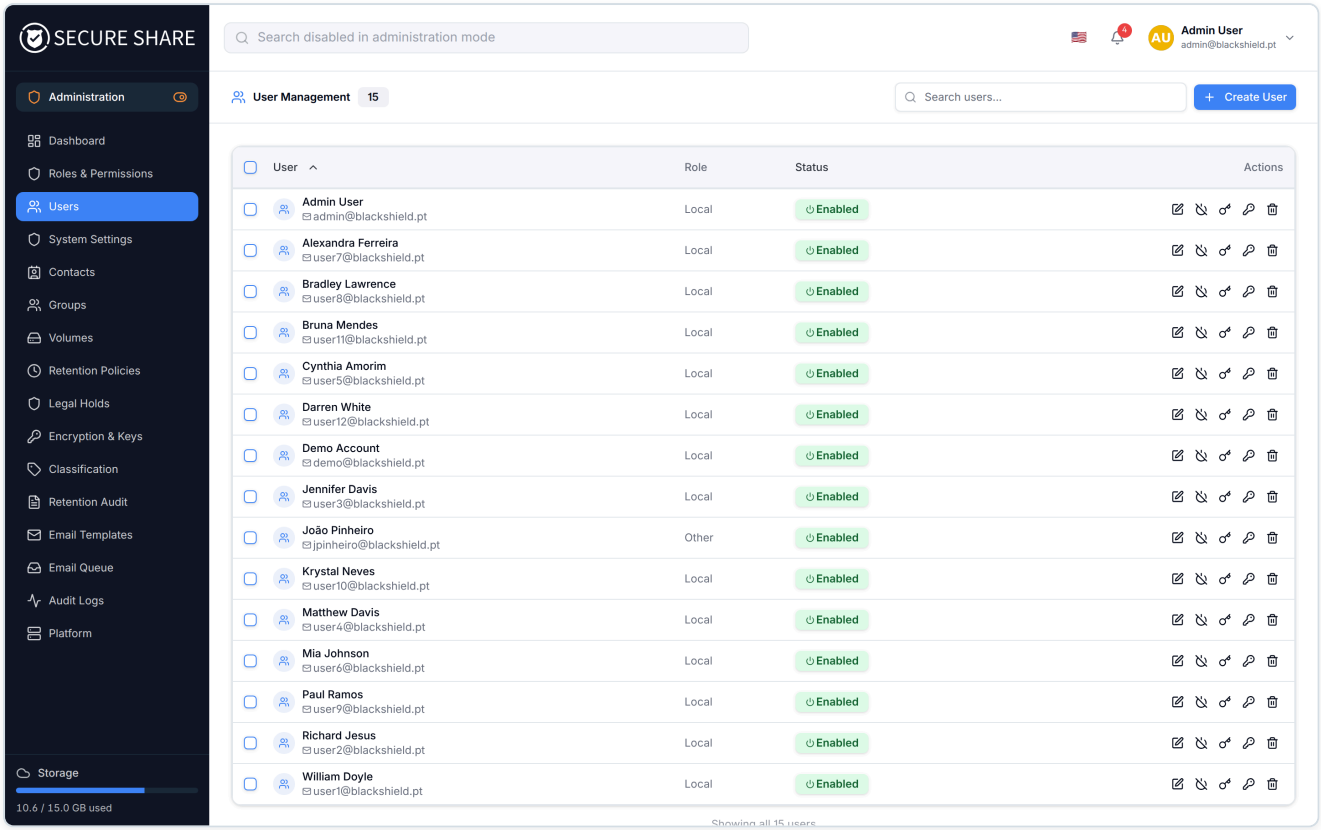
Administrative Control

Administrators get a complete control plane:

- **User management** — provision, enable/disable, force logout, reset, and remove users
- **Roles & permissions** — define and assign granular access
- **Tenant settings** — configure security, storage, features, branding, email, and localization per tenant
- **Quota management** — set and monitor storage limits per tenant and per user
- **Email templates** — customize notifications, password resets, and security alerts
- **Volume management** — manage storage volumes, ownership, and retention defaults
- **License management** — validate licensing and view deployment entitlements
- **Platform statistics** — usage, storage, activity, sharing, and request metrics at a glance



Admin settings — tenant configuration screen



User management screen

11 Productivity & Collaboration

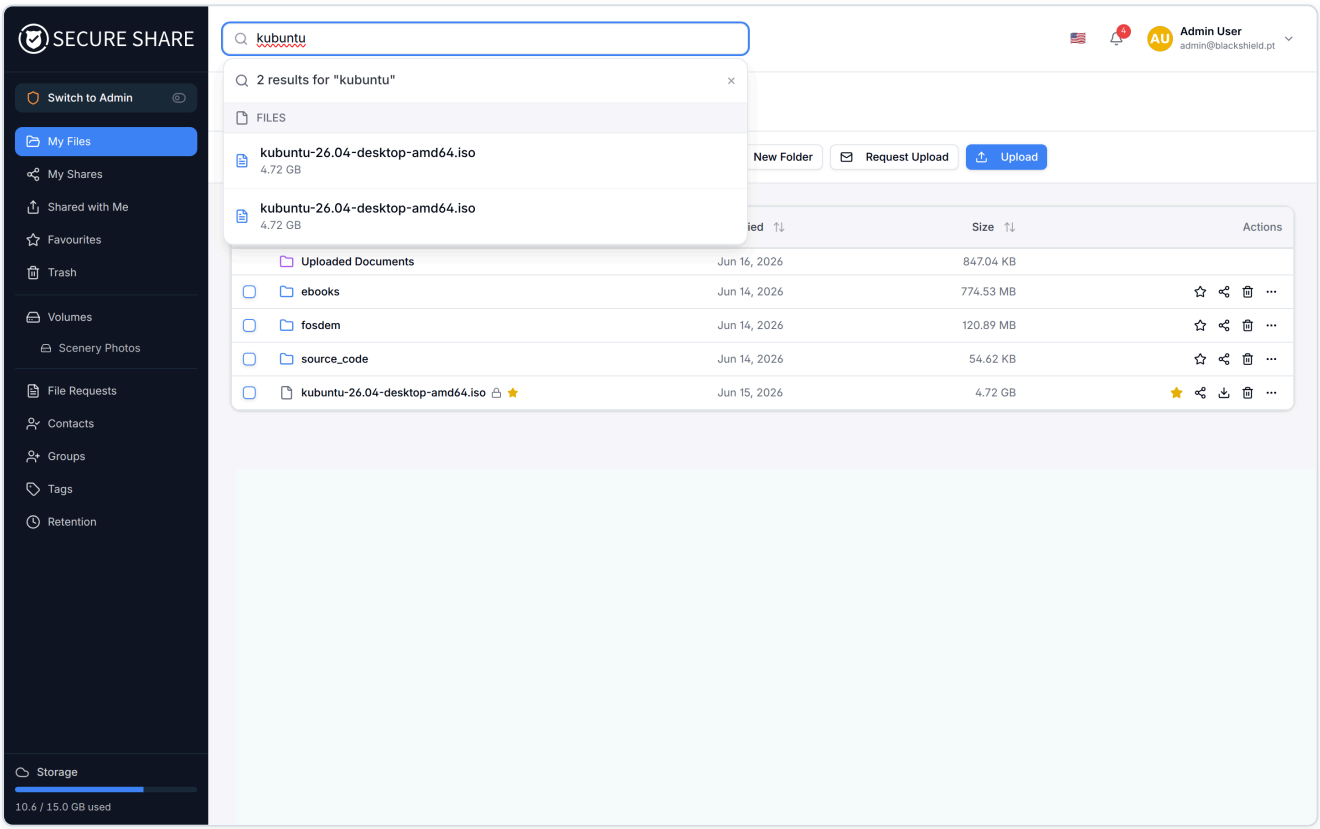
Security shouldn't get in the way of everyday work. SecureShare pairs its encryption and compliance core with the organizational and collaboration tools teams expect.

Organize at Scale

- **Volumes** — top-level storage spaces, each with its own access control, quota, retention defaults, and dedicated inbox and trash. Use them to separate departments, projects, or clients within a single tenant.
- **Folders, tags, and favorites** — structure and label files, and star the ones you reach for most.
- **Trash with restore** — deletions are recoverable from a per-volume trash until they're purged.
- **Unlimited file size** — upload files of any size, with no fixed per-file cap.

Find Anything

Encryption shouldn't make your files harder to find. SecureShare includes **full-text search** powered by a high-performance search engine, scoped strictly to each tenant, so users locate files instantly across their storage.



Search results view with filters

Move Large Files Reliably

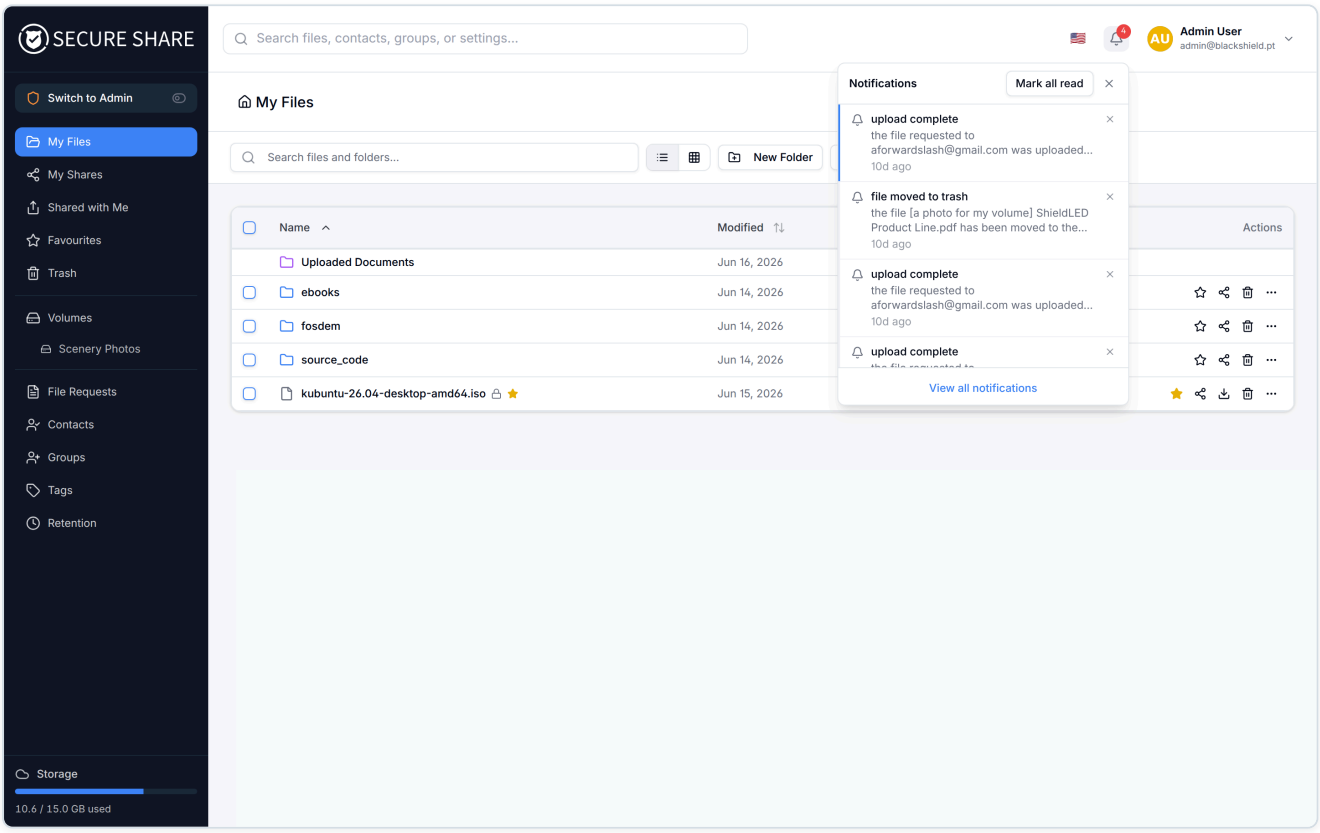
Uploads and downloads are **chunked and resumable**, with progress checkpoints — large files survive flaky connections without starting over. The browser crypto library compresses data before encrypting it, reducing both transfer size and storage footprint.

Stay Informed

A built-in **notification system** keeps users current through in-app and email alerts, with per-category preferences — sharing, uploads, trash, volumes, and security events — so people control exactly what reaches them.

Contacts & Groups

User- and tenant-scoped **contacts and contact groups** make recurring sharing fast: address shares and upload requests to known people and teams instead of re-entering details each time.



Notifications panel and/or contacts management view

12 Architecture & Deployment

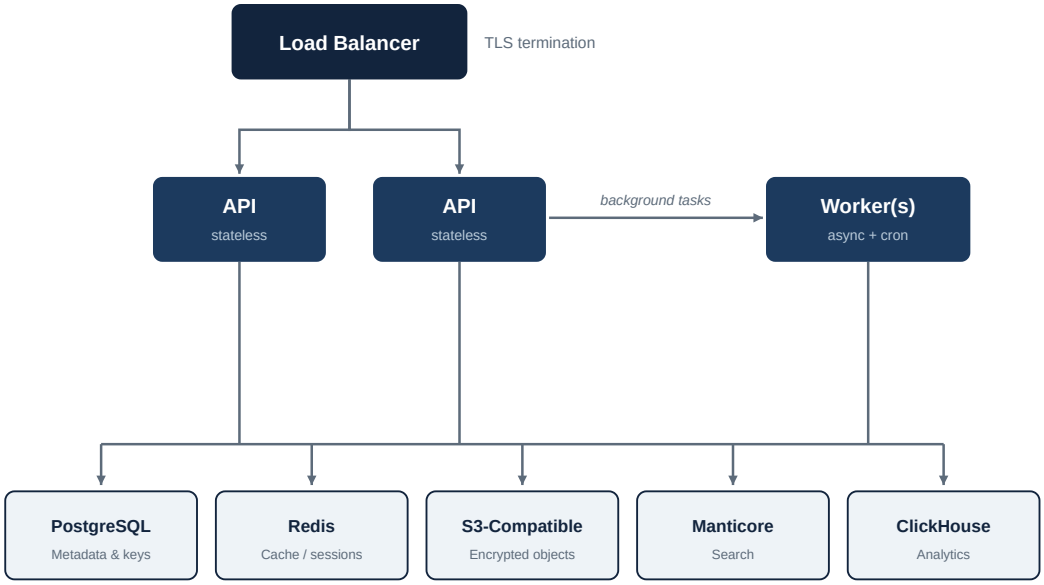
SecureShare is a modern, horizontally scalable platform built on proven open infrastructure.

Technology Stack

Layer	Technology
Web frontend	Modern single-page web application (Vite, Tailwind CSS)
API backend	Python, Flask-based application framework
Primary database	PostgreSQL
Sessions, cache, rate limiting	Redis
Async messaging & background tasks	NATS with JetStream
Object storage	S3-compatible object storage / local filesystem
Full-text search	Manticore Search
Analytics warehouse	ClickHouse
Key management	AWS KMS / OpenBao / environment secrets

Scalable, Resilient Design

API servers are stateless and run behind a load balancer, scaling horizontally for high availability. A dedicated worker tier handles background processing — key rotation re-wraps, retention enforcement, audit warehousing, search indexing, and scheduled maintenance — without impacting interactive performance. Object storage and database tiers scale independently.



© BlackShield

Deployment Options

SecureShare ships with container-based deployment and supports cloud, on-premises, and air-gapped environments. Secrets can be supplied inline or via files and external key-management services, and the platform validates its security-critical configuration at startup to prevent insecure deployments.

© BlackShield

13 Security & Compliance Posture

SecureShare is engineered for environments where security is non-negotiable.

Cryptography

- XChaCha20-Poly1305 authenticated encryption
- Argon2id memory-hard key derivation
- Hierarchical key management with per-tenant rotation
- Native AWS KMS and OpenBao integration

Identity & Access

- MFA (TOTP), OIDC SSO, LDAP/AD
- RS256-signed tokens, encrypted sessions, instant revocation
- Session fingerprinting and new-device alerts
- Adaptive brute-force protection
- Granular RBAC with hierarchical ACLs

Data Protection & Privacy

- Optional zero-knowledge, end-to-end encryption
- Strict multi-tenant isolation
- Anti-enumeration and timing-resistant authentication flows
- Transport security headers (HSTS, frame and content-type protections)

Compliance Enablement

- Retention policies with automated classification *(early access)*
- WORM immutability (governance and compliance modes) *(early access)*
- Legal hold *(early access)*
- Tamper-evident audit trail with SIEM forwarding
- Configurable, long-term audit retention

These capabilities map to many of the technical controls relevant to frameworks such as **GDPR**, **NIS2**, and **DORA**, and standards such as ISO/IEC 27001.

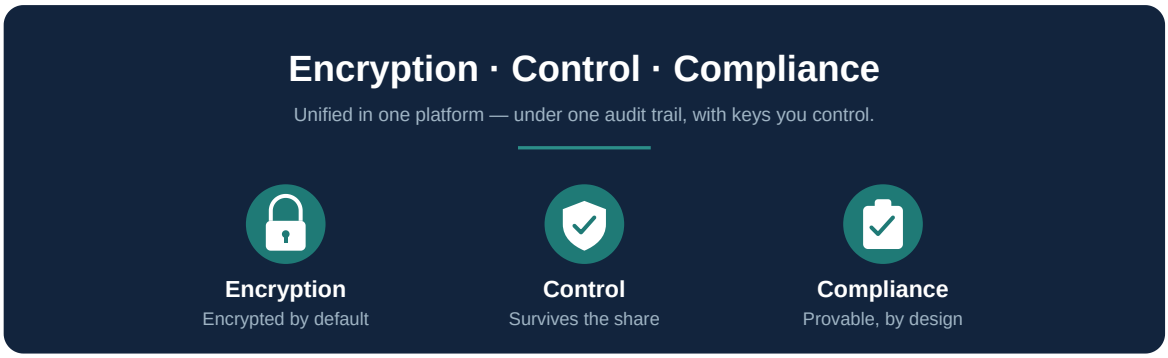
> **Note:** SecureShare provides the technical controls that support compliance. Achieving certification under any specific framework depends on your organization's policies, processes, and deployment configuration.

© BlackShield

14 Why SecureShare

Capability	Consumer cloud storage	Generic enterprise file sharing	SecureShare
Strong at-rest encryption	Sometimes	Yes	**Yes**
End-to-end (zero-knowledge) option	Rare	Rare	**Yes**
Per-tenant key isolation & rotation	No	Limited	**Yes**
Expiring / limited / revocable links	Limited	Yes	**Yes**
Passwordless external upload requests	No	Sometimes	**Yes**
Retention + legal hold + WORM	No	Sometimes	**Yes**
Tamper-evident audit + SIEM	No	Sometimes	**Yes**
Multi-tenant by design	No	Sometimes	**Yes**
Self-hosted / air-gapped option	No	Sometimes	**Yes**

SecureShare brings together encryption, control, and compliance that organizations usually have to assemble from three or four separate products — in one platform, under one audit trail, with one set of keys you control.



Get in Touch

To request a demo or discuss a deployment, contact us at **sales@blackshield.pt**.

BLACKSHIELD

15 Appendix: Glossary & Technical Specifications

Glossary

Term	Meaning
KEK	Key-Encryption Key — a per-tenant key used to encrypt (wrap) file keys, never the file data directly
DEK	Data Encryption Key — a unique, random key that encrypts a single file's contents
WORM	Write Once, Read Many — storage that cannot be altered or deleted for a defined period
TOTP	Time-based One-Time Password — the standard behind authenticator-app MFA codes
OIDC	OpenID Connect — the identity-federation standard used for single sign-on
SIEM	Security Information and Event Management — the security platforms that ingest audit events
AEAD	Authenticated Encryption with Associated Data — encryption that also detects tampering

Technical Specifications

Category	Specification
Symmetric encryption	XChaCha20-Poly1305 AEAD (24-byte nonce, 16-byte authentication tag)
Key derivation	Argon2id (memory-hard; ops=3, 64 MB memory)
Client-side compression	Deflate, applied before encryption to reduce transfer and storage size
Key-wrapping KDF	BLAKE2b-based, domain-separated
Integrity hashing	BLAKE2b per block
Key hierarchy	Master Key → per-tenant KEK (versioned) → per-file DEK
Master key sources	Environment secret, AWS KMS, OpenBao
Token signing	RS256 (asymmetric) JWT access tokens + rotating refresh tokens
MFA	TOTP (RFC 6238) with recovery codes
Federation	OIDC (PKCE + state), LDAP / Active Directory
Encryption models	Transparent server-side · password-protected client-side (zero-knowledge)

© BlackShield

Storage backends	Amazon S3, S3-compatible storage, local filesystem
Database	PostgreSQL
Cache / sessions	Redis
Messaging / tasks	NATS with JetStream
Search	Manticore Search (per-tenant isolation)
Analytics	ClickHouse
Frontend	Single-page web application (Vite, Tailwind CSS)
Backend	Python, Flask-based framework
Large-file transfer	Chunked, resumable upload and download with progress checkpoints
Localization	English, Spanish, French, Portuguese (i18next; extensible)
Deployment	Containerized; cloud, on-premises, and air-gapped

This document is for informational purposes. Feature availability may depend on edition, configuration, and deployment. Specifications are subject to change.

© BlackShield