Vendor Security Overview

1. Role-based access

- Space-level roles: client, view, edit, admin.
- Access checks are enforced server-side for protected actions.

2. Version integrity

- Published versions include deterministic checksum support.
- Public verification links support client-side integrity checks.

3. Audit and governance

- Critical actions are recorded in audit events.
- Immutable audit mode is available for strict governance models.

4. Deployment controls

- Cloud and self-host deployment models are supported.
- HTTPS and security policy controls are configurable.

5. Credential and secret handling

- Passwords and keys are stored as hashes.
- Operational secrets are configured via environment/secret stores.

6. Data ownership

- Tenant-scoped access checks protect artifact boundaries.
- Export and backup flows are available for customer-controlled operations.