SLIDESOURCE®

2026

A Briefing Prepared
by SlideSource

SlideSource Library Security and Governance Overview

A short briefing for IT and security teams evaluating SlideSource Library.

© 2026 SlideSource Inc.

This is a summary, not a full security package. It covers the questions IT teams ask first. Our complete policy set, architecture documentation and assessment results are available on request, and under NDA where appropriate.

What SlideSource Library is

A governed home for scientific presentation content. Slides, presentations, response units and supporting documents live in one controlled library with version history, approval status, evidence traceability and controlled reuse, working alongside the systems your teams already use.

It is delivered as a hosted service on Microsoft Azure.

Hosting and resilience

Resource	Primary	Failover
Web front end	Azure East US	Azure West US
SQL Server	Azure East US	Azure West US 2
Blob storage	Azure East US	Azure West US

- Data is **geo-replicated** from the primary region to the failover regions.
- In a regional outage we can fail over and restore availability **within 60 minutes**, with a **replication delay of approximately 5 minutes**. Data written in the final few minutes before a failover may not carry across.
- Delivered over **HTTPS only**. Data is encrypted in transit and at rest.
- Network access is restricted to what the application requires, and administrative access is restricted further. Specifics are covered in the architecture documentation we provide on request.
- Server infrastructure is patched by Microsoft Azure, with security patches on an accelerated schedule.

Tenancy and separation

The standard deployment is multi-tenant. Customers share infrastructure, and separation is enforced at the library level by three independent mechanisms:

1. **An encrypted access token.** Every request carries a token issued and encrypted with a server-side key, identifying the user and the library they are entitled to. It cannot be tampered with by the client.
2. **Row-level security in SQL Server.** Every table holding customer content is filtered automatically by the database against the library in context. **If that context is not set, no library-specific data can be read or written at all.**

© 2026 SlideSource Inc.

3. **Permission checks in the application**, enforced before content is loaded, by group membership and by individual grant at collection and folder level.

The second layer is deliberately redundant. It exists so that a mistake in application code cannot become a data exposure.

A dedicated instance is available for customers who require complete physical separation from other customers, running on its own infrastructure with its own database, file storage and processing. Connection strings, single sign-on parameters and the site domain are all configured per instance.

Authentication and access

- Every page requires authentication by default. The handful of pages that do not, such as the login and password reset screens, must explicitly opt out, and that list is reviewed.
- Every user has a **unique personal account**. Shared, anonymous and generic accounts are not used.
- **Single sign-on via SAML 2.0** is supported and configured per customer. It can be set as the only permitted route in, so users cannot bypass your identity provider with a local password. Where SSO is used, **your identity provider governs password policy, MFA and account lifecycle**, and removing a user from your directory removes their access.
- **Two-factor authentication** is available for customers not using SSO, and can be applied to administrators only or to all users.
- Where local passwords are used, they are stored as **PBKDF2 hashes with a randomly generated salt** to defeat rainbow-table attacks. Plain text passwords are never stored and cannot be retrieved by us or by anyone else.
- Sessions expire after a period of inactivity, configurable per instance. Users get a **60-second warning** and can extend the session rather than losing work.
- Permissions follow **least privilege**, set per library, per collection, per folder and per group, with individual grants able to override group membership in either direction.

Audit trail

- Changes to content, permissions and configuration are **recorded with the user and timestamp**, and retained rather than overwritten.
- Administrators can review the history of any slide, response unit or document, including who changed what and when, and who approved it.
- Download and distribution activity is recorded, so you can establish what left the library and who took it.

© 2026 SlideSource Inc.

- **Audit events can be exported to your own SIEM** through an authenticated API, so SlideSource activity sits alongside the rest of your monitoring rather than in a silo.
- Azure resource activity is audited separately from application activity.

Content governance

- **Approval workflows** configurable per customer, with the review types you actually use and multiple reviewers where a single sign-off is not appropriate.
- **Version history** retained in full, so you can establish exactly which version of a slide was presented at a given meeting.
- **Lifecycle management**, with review and expiration cycles per content type and alerts before content goes stale.
- **Controlled external sharing.** Content shared outside the organization uses links that can be set to expire, and consultants can be given a read-only view limited to chosen material.
- **Soft deletion** by default, so removals are recoverable.

Data retention and deletion

- Version history and audit records are retained rather than overwritten, because establishing what was presented and when is the point of the system.
- On request we will **permanently delete a library, or all of a customer's data, within one week**. Complete removal from every storage layer can take up to 7 days.
- Because of audit logging and recovery requirements, deleted data may remain recoverable from backups for **up to one year** before aging out.

Optional AI features

- AI features are **off by default** and enabled per library at the customer's choice.
- Where enabled, they run on **Microsoft Azure OpenAI Service in a US region**, under Microsoft's Business Associate Agreement, on a deployment configured so that **content is not retained and is not used to train models**.
- Customer content is not sent to any AI provider unless the customer has turned the feature on.

Development and organizational security

- **Code review of every patch and release**, checking conformance to secure coding practice and guarding against the OWASP Top 10.

© 2026 SlideSource Inc.

- **Microsoft Azure Security Center** monitors the hosted environment for intrusion and surfaces vulnerabilities to address.
- **Vulnerability and penetration testing** under a documented policy, against a dedicated environment.
- A documented information security policy set covering access control, secure development, incident response, business continuity, personnel security, supplier management and acceptable use.
- Staff complete **security and privacy awareness training** and are bound by confidentiality terms.
- We complete customer security assessments and third-party vendor risk assessments, and have been assessed against the ISO 27001:2022 control set.
- Subprocessors are limited and documented. A current list is maintained, provided on request, and governed by the Data Processing Agreement.

What we will provide on request

- Information Security Policy and supporting policy set
- Library Design Document, Data Center Document and infrastructure diagram
- Access Control Management procedure
- Data Backup, Restore and Archival procedure, and the Disaster Recovery Plan
- Secure Development Policy
- Information Security Incident Response Plan
- Vulnerability and Penetration Testing Policy
- SIEM API documentation and SSO Integration Process
- Data Processing Agreement and current Subprocessor List
- Completed security questionnaires, including CyberVadis

Questions from your security team are welcome, and we would rather have them early. Contact us through slidesource.com to request the full documentation set or to arrange a call with the people who build and run the platform.

SlideSource, Inc. Current as of the date of issue, and provided for evaluation purposes. It does not form part of any contract.

© 2026 SlideSource Inc.