

ARCHITECTURE

Connected work. Controlled access.

Standard connects your laboratory operations, measurement records and business documents within a company-scoped workspace.

One company boundary across the workflow

An estimate, work order, instrument, calibration event and issued document belong to a company. The service carries that company context through application requests and database transactions. Laboratories and sites organize the work within that boundary.

A browser workspace backed by transactional services

React and TypeScript provide the browser interface. Kotlin application services use Spring Boot on the JVM, with PostgreSQL for operational records. Versioned database migrations manage schema changes. The browser requests operations; server-side policy decides whether the signed-in person may perform them.

Structured records and document files

Business and calibration records are stored in PostgreSQL. Generated document bytes use object storage, with a company-scoped key and a SHA-256 content digest. The application retains the link between the business record, its document and the version used to produce it.

Authentication, permissions and request protection

Authenticated sessions are bound to company context. API policies apply membership, role or privilege requirements at the server. State-changing requests require the session's anti-forgery token. MetraSlate operator administration uses a separate authorization path from laboratory and customer access.

What this means for your team

The customer conversation, instrument record, technical result and resulting document can remain connected without granting every participant the same access.

TENANT AND CUSTOMER ISOLATION

Keep the right records with the right people.

Company isolation, laboratory permissions and customer access address different layers of the same workflow.

Database row-level security

Tenant-owned tables use PostgreSQL row-level security to check the company identifier on reads and writes. The application's tenant-aware connection layer refuses database access when a required company scope is missing. Company context is applied inside the transaction and cleared before a pooled connection is reused.

Permissions are enforced behind the screen

Server-side policies govern protected operations. Roles and privileges determine what a member may do inside the company. Choosing a laboratory in the interface changes the working view; access policy remains a separate server responsibility.

Asset Light carries the customer and site scope

Customer portal requests carry their customer account scope and, when configured, site grants. A site-restricted contact sees equipment within those grants. An empty grant gives no site access; an instrument without a known site is excluded from a restricted view.

Whole-document access protects every line

A customer document can contain equipment from several sites. For site-restricted access, Standard checks the lines covered by that document. A document containing equipment outside the person's grants is withheld as a whole, so opening a PDF does not reveal another site's instruments.

Real-time conversations have their own checks

Chat subscriptions are checked against company context and channel access before delivery. Client messages enter application handlers; direct client publishing to server broadcast destinations is rejected. An open browser connection does not confer access to every conversation.

Standard uses logical tenant isolation on shared infrastructure. A dedicated database or encryption key for every customer is not implied.

TECHNICAL RECORDS AND AUDIT EVIDENCE

Preserve what supported the result.

A historical calibration needs its original measurement basis, even after procedures, specifications and templates change.

Freeze the result and its basis together

A completed calibration event retains point results and the configuration used to evaluate them. The frozen record includes measurement and uncertainty details, decision-rule context, standards provenance and recorded exclusions. Historical result inspection reads the saved basis instead of silently applying today's configuration.

Database controls protect the frozen record

Frozen calibration-event tables reject updates and deletions through database triggers and application-role permissions. A deferred integrity check verifies that the event's declared included and excluded point counts agree with the rows stored in the same transaction.

Corrections retain the original

A correction is recorded as a successor linked to the earlier event, with a reason. The original event remains available. This provides a traceable explanation of what changed while retaining the earlier technical record.

Review and release are attributable

Technician signature, review approval and quality seal are recorded as distinct actions with an actor and time. Review records identify the document rendering inputs, including template and payload hashes; the seal refers to the review it completes.

Smart documents use published template versions

The Document Creator combines fixed content, branding, typed record bindings and repeating results tables. Validation checks the bindings before publication. Published versions are retained, and generated documents identify their template version. Preview documents are watermarked to distinguish them from issued output.

These controls support traceability and reconstruction of the work. Your laboratory's procedures, authorized signatories and review practices remain part of its quality system.

HOSTED SECURITY AND ASSURANCE

A concrete basis for your security review.

Standard combines application controls with an AWS deployment model for protected data storage and managed service operation.

Protected application entry and storage

The deployment configuration defines HTTPS at the application entry point with TLS 1.2/1.3 support, a PostgreSQL database without public access, and encrypted database storage using AWS KMS. Document storage uses S3 with KMS encryption, versioning and public-access blocking.

Controlled configuration and service operation

Deployment definitions cover managed secrets, application logging, alarms and database backup retention. Backup retention and availability settings are environment-specific. Recovery and availability commitments are established for the service arrangement rather than inferred from a product screenshot.

Technical detail without exposing the implementation

A customer review can examine the tenant boundary, identity and permission model, customer portal scope, document integrity and operational responsibilities. The architecture can be explained through those controls without distributing source code, credentials, database diagrams or internal network details.

SOC 2 and customer assurance

SOC 2 is an independent examination of a service organization's controls. Standard's tenant isolation, authorization, record-integrity and operational controls provide concrete subjects for that review. This product overview does not represent a SOC 2 report or certification.

Bring your laboratory and IT requirements

Contact MetraSlate to discuss your security questionnaire, access model, record-retention requirements and deployment expectations alongside the workflows your laboratory needs.

metraslate.com/contact | SOC framework: AICPA & CIMA