Valutare

CUSTOMER TERMS

Valutare Customer Terms — Security Exhibit

Version 1.0 · Effective December 15, 2026 **Web** valutare.ai/legal/security-exhibit

Preview. These terms take effect December 15, 2026 and may be updated before then.

Binding through Key Terms Part 3.1. It states the measures in place for Customer's instance of the Cloud Service.

#	Measure	In place
1	**Encryption at rest**	Cloud-provider encryption of database storage, object storage and backups; application-level AES-256-GCM encryption of personal-data fields annotated in the data schema; an encryption failure stops the write rather than storing plaintext
2	**Encryption in transit; network**	All external traffic over HTTPS/TLS. The application reaches the database over a private network, and the database has no public IP address
3	**Dedicated instance and tenant separation**	Each customer runs on its own application service and its own database, with its own encryption keys and its own web address. Within that instance, database row-level security and tenant checks in the application remain in place as an additional safeguard.
4	**Access control**	Role-based permissions on every API operation; multi-factor authentication required for all users, including administrators, in customer tenants; sessions expire after 8 hours of inactivity and at an absolute limit of about 24 hours, validated server-side on each request; separation-of-duties controls on compensation changes. Provider personnel use multi-factor authentication for their company accounts and administrative access
5	**Audit logging**	Security-relevant and data-changing operations are logged and integrity-signed; database triggers block changes to audit content and deletion before the retention period ends
6	**Application protections**	Protection against common web attacks, including request-rate limits, strict input validation, cross-site request forgery protection and security headers
7	**Change management**	Automated security testing before changes reach production; staged deployment through development and staging before production, with rollback
8	**AI safeguards**	All AI calls pass through one gateway; automated name detection replaces many personal names before content reaches an AI provider (detection is not guaranteed); each user can turn AI processing off, and Customer's administrators can turn it off for the whole organization in the Cloud Service's settings; AI Output is advisory and labeled in the web application

#	Measure	In place
9	**Backups**	A database backup is taken before every schema-changing deployment, and deployment halts if it fails. Automated daily backups are retained for 30 days, with point-in-time recovery. No multi-region replication is promised
10	**Monitoring**	Error tracking with personal-data scrubbing before transmission; external uptime checks of each customer instance; security and availability alerts paged to on-call personnel through PagerDuty; health checks
11	**Incident response**	Written incident-response and breach-notification procedures; customer notice per Key Terms Part 5
12	**Physical security**	Provided by Google Cloud at its data centers; Provider operates no data-bearing facilities
13	**Personnel**	All personnel with access to Customer Content and Customer Personal Data are bound by written confidentiality obligations before access is granted
14	**Vendors**	Subprocessors bound by written data-protection terms; list and notice per Key Terms Part 5

Assurance status. Provider has not completed an independent security audit or penetration test and is preparing for a SOC 2 examination. Written security documentation and questionnaire answers are available under confidentiality.