

Trust Center

Security, privacy and governance commitments for business use.

Version · October 20, 2026

SHA-256 of source text 76b62edd7984d7f3f5d9b6dd2bb4038c68170331b86a31d9802842fb956ae73a
<https://skyller.ai/en/trust-center/2026-10-20>

1. Our responsibility

Skyller is provided by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, CNPJ **05.699.856/0001-10**, with its registered office at Quadra ACSE 1, Rua SE 1, No. 38, suite 10, 2nd floor, Plano Diretor Sul, Palmas, Tocantins, postal code 77020-014, Brazil.

This center brings together the data protection, security and support commitments governing Skyller's customer relationships. The documents below define rights, responsibilities and channels for assessing your organization's requirements.

2. Documents in this version

- Terms of Use: contracting, acceptable use, AI, billing and liability.
- Privacy Policy: data, purposes, sharing and retention.
- Cookie Policy: common privacy choices across website, signup and platform.
- Data Processing Agreement: instructions, subprocessors, assistance and deletion.
- Integrated services: potential recipients according to the workflow used.
- Data protection and your rights: requests, criteria and applicable deadlines.

Each document has an identified version and integrity hash. Skyller will preserve the reference to the text associated with each acceptance, allowing consultation during the contractual relationship and afterwards where needed to exercise legal rights.

3. Protection commitments

Area	Contractual commitment
Access	Restrict processing to authorized people and services, with permissions appropriate to their roles
Data protection	Adopt technical and organizational measures proportionate to risk and contracted scope
Confidentiality	Require confidentiality duties for people authorized to process data
Incidents	Notify customers and cooperate in investigation and mitigation under the DPA
Providers	Establish protection obligations, oversee processing and communicate subprocessor changes
Rights and deletion	Provide assistance and coordinate return or deletion under instructions and applicable law

Customers must manage users, credentials and sharing, restrict agent permissions and review consequential actions and outputs. These duties complement, rather than replace, Skyller's obligations.

Skyller and the model API providers it selects and contracts do not use customer inputs — including prompts, messages and documents — or generated outputs to train artificial intelligence models. This commitment covers Skyller model routes, including fallback. Processing needed to respond and operational retention follow the Privacy Policy and DPA. Independent services contracted directly by the customer are governed by their own conditions.

4. Service conditions and specific requirements

Service levels, support hours, data residency and specific retention periods will be defined in expressly contracted conditions. Support will assist in assessing these requirements and identifying the features and providers involved.

For regulated uses or sensitive data processing, the parties must assess purposes, data categories, instructions and additional safeguards before starting the relevant workflow.

Skyller will provide information about measures applicable to processing and cooperate in assessments and audits under the DPA. Return and deletion will cover data within its responsibility and coordination with subprocessors, subject to legal retention and protected backup cycles.

5. International use

Portuguese, English and Spanish versions provide a common contractual basis while preserving mandatory rules applicable to the circumstances. Additional territorial or sector-specific requirements may be addressed in the service's specific conditions.

Each version provides the full content in its language. Contract interpretation rules appear in the Terms and DPA, subject to applicable mandatory law.

6. Privacy, security and support

Send contractual questions to contact@skyller.ai, privacy requests to privacy@skyller.ai, and vulnerability reports or suspected incidents to security@skyller.ai. Describe the context without sending passwords or secrets. The team may verify identity and authorization before sharing restricted information.

Intrusive testing requires prior authorization. Business assessments may request additional information about controls, processing contracts and suitability for their needs through the same channel.