Security Annex

Version 1.0 · Effective date: November 4, 2026

Northbyte Inc. · 2880 Zanker Rd., Suite 203, San Jose, CA 95134

https://gonovus.ai/legal/security/v1.0

This Security Annex describes the security measures GoNovus maintains for the Service under Section 9.2 of the MSA (https://gonovus.ai/legal/msa) and Section 8 of the DPA (https://gonovus.ai/legal/dpa). GoNovus may update these measures from time to time, provided that updates do not materially reduce the overall security of the Service. Each update is posted here with a new version number and date.

Governance

Written information security policies approved by the CEO and reviewed at least annually; designated Security Operations Lead; annual risk assessment and Board briefing; control monitoring through Vanta; SOC 2 program aligned with AICPA Trust Services Criteria.

Personnel

Confidentiality agreements; background checks where permitted by law; security awareness training at onboarding and annually; policy acceptance; prompt access removal at offboarding.

Access control

Role-based, least-privilege access; SSO and multi-factor authentication for production and administrative systems; unique accounts; access approval and quarterly access reviews; logical separation of customer data.

Encryption

TLS 1.2+ for data in transit; AES-256 encryption at rest using Azure-managed keys; secrets stored in a managed key vault.

Infrastructure

Hosted on Microsoft Azure in the hosting region stated in the Order Form (default: United States regions only); network segmentation and firewalls; hardened configurations; Azure physical and environmental controls (Azure SOC 2 / ISO 27001).

Secure development and change management

Code review and approval before production; separate development and production environments; documented emergency change process with after-the-fact review; dependency and vulnerability scanning.

Vulnerability management

Regular vulnerability scanning and patching by severity; penetration testing when scheduled; public vulnerability reporting address.

Logging and monitoring

Centralized logging of security-relevant events; alerting on suspicious activity. Log retention follows the fixed periods in Data minimization, retention and deletion below.

Incident response

Documented incident response plan with roles, escalation, and customer notification without undue delay and in any event within 72 hours after becoming aware of a Security Incident, as defined in the DPA; post-incident review; annual testing.

Business continuity

Automated backups with encryption; backup restoration testing at least annually; commercially reasonable efforts to restore the Service following an interruption (no numeric RTO/RPO commitments).

Vendor management

Security review of Subprocessors before onboarding and periodically after; written data protection terms.

AI-specific controls

No training on Customer Data; contractual no-training terms with AI model providers; prompt and output guardrails; per-customer configuration isolation; monitoring of AI Output quality.

Data minimization, retention and deletion

Collect only data needed for the Service.

We apply the fixed retention periods set out below. They are not configurable by merchants. Copying, retrying, or saving information again does not restart the applicable retention period. A shorter applicable retention period or legal deadline takes precedence, except where the law requires us to retain necessary records.

Information	Retention and conditions
Merchant accounts and store configuration	We retain this information only for as long as necessary to provide the services. When authorization is revoked or the app is uninstalled, we stop using and delete the corresponding credentials. Information that is no longer necessary is deleted under the arrangements below.
Chat messages, including text chat and voice interactions (audio and voice transcripts)	We retain messages online for 90 days from creation. Attachments expire with their associated messages. Summaries do not extend the retention period of the original information.
Order query snapshots and copies	We retain these for 24 hours from when the original query results are obtained. This limit also applies to copies in logs, backups, and other systems.
Unsent drafts that have not been finalized	We retain these for 7 days from the customer’s last edit.
Support requests and email records	Records held by GoNovus or its service providers are retained for no more than 12 months from creation of the original request. This includes email copies and delivery records. Copies already delivered to a merchant’s own mailbox are managed by the merchant under its own privacy practices.

Information	Retention and conditions
Technical, security, and support records	We retain AI debugging records online for 7 days, operational logs for 10 days, and technical request metadata that excludes message content for 30 days. Each period begins when the underlying event first occurs or the record is first generated. Access and sensitive-operation audit records are retained for no more than 180 days from the event. These audit records contain only necessary operational information and exclude conversation content, order content, and credentials. An applicable earlier deletion deadline takes precedence, except where the law requires us to retain necessary records. AI service providers' own retention practices are addressed separately in Section 6.2 of the Product Privacy Policy at https://gonovus.ai/privacy.
Backups	We retain regular business backups on a rolling basis for 14 days from creation of each backup. After deletion from online systems, any residual copies in isolated backups are retained for no more than 21 days, including any additional recovery period. A shorter data-specific limit takes precedence; in particular, the 24-hour limit for order query snapshots also applies to backup copies. When restoring a backup, we apply existing deletion requirements before making the restored data available for use.

Uninstalling the app revokes access for that installation but does not immediately erase all previously stored information. Uninstallation, a determination that information is no longer necessary, or a valid deletion request triggers deletion before the normal retention period expires. We aim to delete online copies within 7 days of the triggering event and complete deletion of all applicable copies within 30 days. A shorter retention period or legal deadline takes precedence, except for necessary records that must be retained by law.

Deletion covers relevant GoNovus systems and applicable copies held by our service providers. Copies already delivered to a merchant's own mailbox remain under the merchant's control. A delay in receiving an uninstall notification does not extend the deletion deadline measured from uninstallation. Reinstalling the app does not cancel deletion of the previous installation's data, and that deletion does not remove data associated with the new installation.

Where information must be retained to comply with legal requirements, we restrict its use and delete or irreversibly anonymize it when the basis for retaining it no longer applies.