



# Published security and privacy policies

Version 1.0 | Effective October 11, 2026

ARA Management Group / Venduli

Reporting: [security@venduli.store](mailto:security@venduli.store)

Web: <https://venduli.store/privacy/request>

## Policy requirements and implementation status

Publication establishes requirements; it does not establish that every organizational control is implemented. The platform owner is accountable until delegates are named. No formal DPO appointment or independent certification is claimed. Mailbox delivery and monitoring require owner verification.

Application controls include management MFA, one-use recovery codes, inactivity re-verification, store isolation, encrypted integration tokens, privacy-request registration, and customer account-profile export/deletion. Endpoint security, cloud IAM/MFA, network segmentation, comprehensive contract-end erasure and backup deletion, response staffing, and external notification delivery require separate completion and verification.

# Venduli Privacy Policy

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Operator and contact

Venduli is operated by ARA Management Group. For privacy requests or security concerns, contact [security@venduli.store](mailto:security@venduli.store) or use our privacy request form. Store merchants operate their own storefronts and are responsible for their own customer communications and privacy notices.

## Information we process

We process merchant and customer account details, store configuration, product and order information, shipping addresses where provided, support and privacy requests, authentication records, and security logs. When a merchant authorizes TikTok Shop, we store authorization tokens and seller identifiers for that merchant's store. TikTok product and order synchronization is not enabled yet. We do not store raw payment card numbers or CVV.

## Why we process it

We use information to provide stores, authenticate users, manage enabled commerce and shipping features, support merchants, respond to requests, prevent abuse, and meet applicable obligations. We do not sell customer personal data. TikTok information is used only for authorized integration functions, not unrelated advertising or model training.

## Providers and locations

Services may involve Microsoft Azure hosting and databases, Cloudflare delivery and asset storage, Stripe payments, authorized shipping carriers, and TikTok Shop. The application is hosted in Azure Central US, United States. Cloudflare and other providers may process traffic or service data in additional countries according to their services and configurations; a complete location inventory is still being verified. We do not represent that every category is stored exclusively in the United States.

## Cookies and marketing

Session cookies support sign-in and account security. Storefront features may use browser storage for preferences, favorites, carts, and popup display frequency. Merchants must disclose any additional analytics or marketing integrations they enable. Creating an account does not itself authorize promotional email or SMS.

## Retention and deletion

We retain data for the service purpose and applicable obligations. Our contract-end deletion procedure targets removal from active systems within 30 days of a verified instruction, subject to documented obligations or holds. Backup expiration and deletion must be verified against provider settings. Our app does not yet automatically erase all orders, carrier records, third-party data, and backups. Customer self-service export and deletion cover their registered account profile and sessions; order records are handled through a separate verified request.

## Your requests

Use the request form for access, correction, deletion, or questions. We verify identity proportionately and coordinate with the relevant merchant. We do not release records solely because someone supplies an email address. We target acknowledgment within five business days and response within 30 days, subject to applicable requirements. Requests are saved for owner review; the form does not automatically email a confirmation.

## Security and accountability

We use store-scoped access checks, password hashing, encrypted integration-token storage, HTTPS, and required authenticator verification for management access. These measures reduce risk but do not guarantee against every incident. No independent ISO, SOC 2, or ePrivacy certification is claimed, and no formal Data Protection Officer has been designated.

## Updates

This policy is version 1.0, effective October 11, 2026. We review it quarterly and after material service changes. The next scheduled review is January 11, 2027. Material revisions will be published with their effective date.

# Information Security Policy and Program

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Purpose and scope

Protect the confidentiality, integrity, and availability of Venduli information. Applies to ARA Management Group personnel, contractors, company endpoints, Azure infrastructure, Cloudflare services, merchant data, and authorized TikTok Shop data.

## Governance

The platform owner approves this program, appoints a Security Lead and Privacy Lead, funds controls, and reviews risk quarterly. One person may hold multiple operational roles, but high-risk access and exceptions require recorded owner approval. The platform owner is accountable for these roles until named delegates are recorded in the governance register.

## Required safeguards

Maintain inventories of systems, owners, vendors, data flows, and processing countries. Apply the daily security baseline, least privilege, encryption, vulnerability management, incident response, and deletion procedures in this package. Collect only necessary data. Separate production from development and use synthetic test data.

## Risk management and assurance

Record each risk with impact, likelihood, owner, treatment, evidence, and review date. Assess vendors before sharing personal data and review annually. Review access quarterly; test backup restoration and incident response at least annually. Keep evidence of training, reviews, scans, remediation, and approved exceptions.

## Publication and review

Publish approved internal policies in a staff-accessible controlled repository. Publish the approved customer privacy notice on the website. Review this program annually and after material changes or incidents. A written policy is not evidence that every safeguard is operating.

# Daily Operations Security Baseline

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Endpoints and workspace

Use supported operating systems with automatic security updates, active endpoint protection, full-disk encryption, and a managed device inventory. Lock screens automatically within five minutes and whenever unattended. Remove sensitive papers from desks; secure or shred them. Do not use shared public computers for administration.

## Passwords and MFA

Use unique passwords of at least 15 characters for workforce accounts where supported, generated and stored in an approved password manager. Block commonly compromised passwords where supported. Do not share accounts or credentials; change passwords following compromise. Require MFA for email, Azure, Cloudflare, source repositories, and privileged application access; prefer passkeys or security keys. Venduli management access requires an enrolled authenticator or one-use recovery code. Management verification expires after 30 minutes of inactivity. Cloud-account MFA must be configured separately.

## Daily operations

Check security alerts each business day and escalate suspicious events immediately. Do not email secrets or put them in chat, screenshots, source code, or tickets. Verify unusual payment, access, and data-export requests through a second channel. Keep recovery codes in a controlled vault.

## Network baseline

Restrict administrative interfaces, database access, and service credentials to necessary identities and systems. Use firewall rules and segmented production/development environments. Enable and test relevant network, identity, and application monitoring. HTTPS and a cloud provider account alone do not establish network segregation.

## Verification

Record device encryption and antivirus status, screen-lock configuration, MFA enrollment, approved access paths, update status, and monitoring tests before claiming implementation. Train personnel at onboarding and annually.

# Access Control and Least Privilege Policy

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Access approval

Every account must have an identified owner and business need. The system owner approves access before provisioning. Use separate named accounts for ordinary work and elevated administration where supported. Grant minimum role, resource scope, and duration; deny access by default.

## Store isolation

Merchant users may access only stores assigned to them. Customer identities and sessions must be scoped to their store. Validate authorization server-side for every sensitive action and query. Never trust a client-supplied store identifier without permission checks. Privileged support access requires a ticket, justification, and audit trail.

## Personal data and production

Production database access is limited to approved operational roles. Developers use synthetic data by default. Exports require approval and documented destination and deletion date. Do not use production customer data for unrelated marketing or testing.

## Lifecycle and reviews

Remove access immediately on departure or suspected compromise and within one business day of role change. Review workforce and service accounts quarterly. Expire temporary access automatically where possible. Rotate service credentials after compromise or ownership changes. Record access grants, removals, reviews, and exceptions.

## Evidence

Maintain an access register listing person/service, role, approved stores/resources, approver, MFA status, grant date, review date, and revocation date. Current code supports store authorization checks; this does not verify company-wide cloud IAM or MFA.

# Data Classification and Encryption Policy

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Classification

Public: approved marketing and storefront images. Internal: operational procedures and non-sensitive metrics.

Confidential: merchant/customer names, email, phone, addresses, orders, support messages, and non-public commercial data. Restricted: API secrets, OAuth tokens, encryption keys, password hashes, identity documents, and payment credentials. Do not store raw card numbers or CVV.

## Handling

Data owners assign classifications and review when purpose changes. Public R2 storage may contain only approved public assets. Never upload shipping labels, identity documents, customer exports, or secrets to a public bucket. Confidential and Restricted data require authenticated access and minimum necessary sharing.

## Encryption requirements

Require TLS 1.2 or later for personal-data transport and verify server certificates. Verify provider encryption at rest for databases, object storage, disks, and backups. Require full-disk encryption on workforce devices. Application secrets and TikTok tokens must use authenticated encryption; Venduli currently uses AES-256-GCM for stored integration tokens.

## Key management

Restrict key access independently of data access where possible. Store keys in a managed secret store, not source code. Record key owners, rotation plans, recovery process, and access reviews. Rotate on compromise. Document safe re-encryption and rollback before planned rotation.

## Evidence and limitations

Retain provider configuration exports proving at-rest encryption and backup protection. Code inspection confirms token encryption and certificate-verifying database connections when TLS is configured; database, backup, endpoint, and R2 encryption settings must still be verified.

# Incident Response and Breach Notification Procedure

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Roles and channels

Security Lead: triage, containment, evidence, and recovery. Platform Owner: resources and escalation. Privacy Lead: personal-data impact and notification decisions with qualified advice when needed. Communications Lead: seller and TikTok updates. The platform owner coordinates response until delegates and a backup contact are recorded. Intake: security@venduli.store, subject SECURITY INCIDENT; delivery, monitoring, and an urgent backup phone channel must be verified by the owner.

## Triage targets

These are internal targets, not legal deadlines: escalate suspected personal-data exposure immediately; begin critical-incident triage within one hour of receipt; notify the owner within two hours. Provide an initial affected-seller/TikTok notice within 24 hours after identifying a credible impact, or sooner where a binding requirement applies. Do not delay initial notification while waiting for complete forensic certainty.

## Response steps

Open an incident record with discovery time, reporter, systems, suspected data, and severity. Preserve logs and evidence with access controls and a chain-of-custody record. Contain affected accounts, integrations, and hosts; revoke/rotate compromised tokens. Investigate scope and affected stores. Remediate root cause, verify recovery, and monitor for recurrence.

## Notification decision

Evaluate suspected and confirmed personal-data exposure promptly. Identify applicable contracts and legal requirements, responsible recipients, and deadlines; do not assume one universal deadline. Send notices via verified seller contacts and TikTok Partner Center support or designated contractual channel. Track delivery, updates, and decisions not to notify.

## Notice contents and follow-up

Include incident reference, discovery and occurrence times if known, affected systems/data/stores, known impact, containment, recommended actions, contact, and next update time. Avoid speculation and unnecessary personal data. Update at least daily during an active critical incident. Complete a lessons-learned review within ten business days after closure and conduct an annual tabletop exercise.

# Vulnerability and Threat Management Procedure

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Discovery

Inventory deployed applications, dependencies, cloud resources, and endpoints. Review vendor alerts and threat notices weekly. Scan dependencies and secrets before release and at least weekly; scan production exposure at least monthly. Test authentication, authorization, store isolation, and file upload paths after significant changes.

## Prioritization targets

Internal remediation targets: actively exploited or exposed critical issue - contain within 24 hours; critical - fix within 7 days; high - 14 days; medium - 30 days; low - 90 days. Prioritize exploitability, personal-data exposure, and internet reachability over score alone.

## Remediation workflow

Create a ticket with discovery date, affected assets, severity, owner, deadline, mitigation, and evidence. Test fixes before deployment, use rollback plans, verify after release, and close only after retest. Owner-approved exceptions require compensating controls, expiry, and periodic review.

## External reporting

Use the verified security intake channel in the incident procedure. Acknowledge reports within two business days. Do not promise a bug bounty or authorize intrusive testing without a written scope. Never include customer records or secrets in public vulnerability tickets.

## Evidence

Keep scan summaries, dependency updates, patch records, remediation tickets, retest results, and exception decisions. Tests currently exist in the repository; continuous scanning, alerting, and independent penetration testing are not established by those tests alone.

# Internal Personal Data Protection Policy

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Scope and accountability

The Privacy Lead maintains a processing register covering purpose, data categories, sources, store scope, recipients, physical processing locations, safeguards, retention, and request handling. Clarify controller/processor responsibilities in merchant agreements; do not assume one role for all processing.

## Minimization and use

Collect only information needed for store accounts, orders, shipping, support, and authorized integrations. Do not sell customer data or reuse TikTok data for unrelated advertising, profiling, or model training. Review new processing and vendors before launch. Assess consent and other applicable requirements for marketing separately.

## Requests

Receive requests through a verified privacy contact. Log the request, verify identity proportionately, identify the responsible merchant, and securely assist with access, correction, deletion, or other applicable requests. Do not expose one store's records to another. Target: acknowledge within five business days and resolve within 30 days unless a shorter applicable requirement controls.

## Sharing and locations

Approve subprocessors and maintain contracts and location records. Azure application deployment is in US Central US; database, Cloudflare object-storage location, global edge processing, logs, and backups require separate confirmation before answering country questions. Explain transfers accurately in notices and contracts.

## Review

Review quarterly and following material processing changes, new integrations, incidents, or legal changes. Train personnel annually. Maintain request, vendor, retention, incident, and review registers. Record exceptions and unresolved implementation gaps.

# Data Retention and Contract-End Deletion Procedure

Version 1.0 | Effective October 11, 2026 | Accountable owner: platform owner

## Schedule ownership

Privacy Lead and system owners approve a category-specific schedule before adoption. Record legal/contract basis and retention period for accounts, orders, shipping labels, support tickets, logs, OAuth records, and backups. Operational targets below require engineering verification and documented exceptions where not yet met.

## Contract termination

Verify requester authority and record the effective end date. Revoke integration authorization, access, and tokens promptly. Offer any contractually permitted secure export before deletion. Delete customer personal data in active systems within 30 days after the authorized termination/deletion instruction, except specifically justified obligations or holds.

## Deletion coverage

Inventory and remove relevant records from database tables and settings, private objects, labels, exports, caches, logs where appropriate, test copies, and subprocessors. Apply deletion by store ID with authorization and a dry-run report. Do not remove data belonging to another store. Public product assets and transaction records also require an explicit retention decision.

## Backups and exceptions

Delete backup copies when their verified retention cycle expires; policy maximum is 90 days, subject to actual provider configuration and contract. Prevent ordinary use of retained backup data. If restored, reapply deletion records. Legal holds must have a reason, narrow scope, authorized owner, review date, and documented eventual deletion.

## Verification and seller communication

Verify deletion with counts and targeted queries; record systems, completion dates, exceptions, backup expiry, and reviewer. Provide an accurate deletion confirmation that describes retained categories and reasons. Do not promise all data is gone immediately when backups or obligations remain. Current application deletion workflows and backup purge controls still require implementation.