vz labs

Security Overview

TRUST CENTER DOCUMENT | CHÂTAIGNE

DOCUMENT	Security Overview
VERSION	v1.0 · SEC-OVW-001
DATE	26 MAY 2026
OWNER	VZ Labs SA
PRODUCT	Châtaigne
REVIEW	Annual and upon material security program changes

This Security Overview summarizes Châtaigne’s current security practices for protecting restaurant, customer, and operational data across the Châtaigne platform.

Châtaigne enables restaurants to receive and manage direct orders through messaging channels such as WhatsApp and Instagram. The platform processes operational data needed to answer customer questions, create orders, coordinate payment and fulfillment, and provide restaurant support.

1. SCOPE

This overview covers the Châtaigne application, production infrastructure, employee access practices, software development lifecycle, incident response process, and vendor security approach.

This document is intended for Trust Center and audit-readiness use. It is informational and does not replace the terms of any signed customer agreement.

2. DATA PROTECTION

2.1 Encryption

- Customer and operator traffic is protected in transit using TLS where supported by the relevant application and provider endpoints.
- Production data is stored using managed cloud and database providers that support encryption at rest.
- Payment card processing is handled by dedicated payment processors. Châtaigne does not intentionally store full payment card numbers or card verification codes.

2.2 Data minimization and handling

- Châtaigne collects and processes data needed to operate ordering, support, payment, delivery, and restaurant workflows.
- Access to production data is limited to authorized personnel with a business need.
- Sensitive secrets and credentials are managed through a secrets management system and are not intentionally committed to source code.

3. ACCESS CONTROL

- Production and administrative access is restricted to named accounts and assigned according to role and business need.
- Multi-factor authentication is required or expected for critical systems where supported by the service.
- Administrative privileges are limited to personnel who require them to operate or support the platform.
- User access is reviewed periodically and access is removed or updated when personnel change roles or leave the organization.

4. INFRASTRUCTURE SECURITY AND RESILIENCE

- Châtaigne uses managed cloud infrastructure and specialized service providers for hosting, databases, messaging, payments, observability, and supporting business operations.
- Production systems are separated from local development and test workflows through environment configuration, access controls, and provider-level permissions.
- Logging, monitoring, and alerting are used to detect operational errors, availability issues, and security-relevant anomalies.
- Backups and managed-provider resilience features are used to support recovery objectives for critical data and services.

5. SECURE DEVELOPMENT PRACTICES

- Application changes are developed through source control and reviewed before being merged into production branches.
- Automated checks, testing, and build verification are used where appropriate to reduce regression risk.
- Security-sensitive changes are reviewed with attention to authentication, authorization, data handling, logging, and provider integrations.
- Dependencies and runtime services are monitored through provider tooling and internal review processes.

6. INCIDENT RESPONSE

Châtaigne maintains an incident response process intended to identify, triage, contain, remediate, and learn from security and availability incidents.

- Incidents are assessed for severity, customer impact, data sensitivity, and regulatory or contractual notification requirements.
- Relevant personnel coordinate containment, remediation, customer communication, and provider follow-up.
- Material incidents are reviewed after resolution to identify root cause, corrective actions, and prevention measures.

Security concerns may be reported through the Châtaigne Trust Center or by contacting support@chataigne.ai. Availability incidents and maintenance updates can be viewed and subscribed to at status.chataigne.ai.

---

7. VENDOR MANAGEMENT

- Châtaigne relies on third-party providers for cloud hosting, data storage, messaging, payments, delivery, AI processing, observability, and internal business operations.
- Vendors are reviewed based on the nature of the service, access to sensitive data, business criticality, and available security/compliance documentation.
- High-impact vendors are periodically reviewed and tracked as part of the security and compliance program.

8. COMPLIANCE POSTURE

- Châtaigne is preparing for SOC 2 Type 1 and maintains security program documentation, evidence, and control ownership in Vanta.
- Châtaigne’s privacy and data handling practices are designed with GDPR and Swiss data protection expectations in mind.
- Where applicable, customer data processing terms and vendor commitments are reviewed through legal and security processes.

9. REVIEW AND OWNERSHIP

This document is owned by the CTO and reviewed at least annually. It is updated when there are material changes to Châtaigne’s platform, security program, vendor posture, or compliance status.

Current owner: VZ Labs SA. Current review date: 26 May 2026.