Veros Trust Center: Security Overview

Security is not an add-on at Veros.
It is built into how we design, develop, and operate the platform.

We process business-critical trade and compliance data.
We treat it accordingly.

For security-related inquiries: security@veros.ai

1. Security Governance

Security responsibility sits at leadership level.

Our Chief Technology Officer is accountable for:

- Secure system architecture
- Infrastructure protection
- Application-level security controls

Security practices are embedded into development workflows, infrastructure management, and vendor selection.

Our security framework evolves as we grow, and as customer and regulatory expectations increase.

2. Infrastructure & Hosting

The Veros platform is hosted on Amazon Web Services (AWS) within the European Union.

We do not operate on-premise servers.

AWS provides enterprise-grade physical and environmental security, including:

- Controlled facility access
- 24/7 monitoring
- Redundant power and environmental safeguards
- Secure hardware lifecycle management

AWS maintains internationally recognized certifications and independent audits, including:

- ISO 27001
- ISO 27017
- ISO 27018
- SOC 1 and SOC 2

These certifications cover the underlying cloud infrastructure and data centers.

Veros remains fully responsible application-level security, logical access control, encryption and data protection.

Detailed infrastructure documentation is available under NDA upon request.

3. Data Encryption

Customer data is encrypted:

- At rest using industry-standard AES-256 encryption
- In transit using TLS 1.2 or higher

Encryption keys are managed using controlled key management services with strict access policies and audit logging.

Encryption standards apply across production and non-production environments.

4. Access Control & Authentication

Access to Veros is governed by strict authentication and authorization controls.

Key measures include:

- Unique user accounts
- Strong password requirements
- Multi-Factor Authentication support
- Mandatory MFA for Veros staff accessing production systems
- Role-Based Access Control
- Logical tenant separation

Customer databases are not directly accessible to users.

Administrative access is restricted, logged, and periodically reviewed.

5. Secure Software Development

Security is integrated into our development lifecycle.

Our practices include:

- Controlled source code repositories with enforced authentication
- Peer-reviewed pull request workflows
- Automated testing prior to deployment
- Segregation between development and production environments
- Fully logged deployment processes
- No direct shell access to production systems

Security updates and dependency patches are monitored continuously and validated before release.

6. AI Data Protection Standards

Where AI functionality is used within Veros:

- Customer data is processed solely for the defined functional purpose
- Customer data is not used to train or fine-tune AI models

- AI processing operates in stateless or isolated inference modes
- Data remains encrypted in transit and at rest
- Access to AI environments is restricted and logged

Our AI philosophy is clear. AI enhances expertise. It does not replace accountability.

7. Monitoring & Logging

We implement centralized monitoring and logging to support:

- Security oversight
- Anomaly detection
- Operational diagnostics
- Traceability of user actions

Sensitive data is not logged in plaintext.

8. Incident Management

Veros maintains a formal incident response framework covering:

- Detection
- Containment
- Investigation
- Remediation

Where a confirmed security incident affects customer data, affected customers are notified without undue delay.

Where personal data is involved, we apply additional procedures in line with GDPR and our documented breach response framework.

All incidents undergo root cause analysis and corrective action.

9. Business Continuity & Backup

Customer data is backed up using encrypted, automated AWS-managed backup mechanisms within the European Union.

Backups are designed for disaster recovery and are not used for active processing.

Recovery procedures are defined and reviewed periodically as part of our governance program.

10. Vendor & Subprocessor Management

We apply a risk-based vendor assessment approach.

Where third parties process customer data:

- Written data protection agreements are in place
- Encryption and access controls are required

- International transfer safeguards are implemented where applicable

An up-to-date subprocessor list is available upon request.