Veros Security Overview

1. Security Governance

Security at Veros is embedded into our architecture, development lifecycle, and leadership oversight.

Responsibility for technical security controls, secure architecture, and infrastructure protection rests with the Chief Technology Officer (CTO). Security practices are integrated into product development, infrastructure management, and vendor selection.

Security is reviewed regularly and evolves proportionally with the company's growth and risk profile.

All external security communication can be directed to:

security@veros.ai

2. Infrastructure & Hosting

The Veros platform is fully cloud-native and hosted on Amazon Web Services (AWS).

Primary hosting region:

EU-West-3 (Paris, France)

Veros does not operate on-premise servers.

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

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

AWS maintains independently audited, internationally recognized security certifications and attestations, including:

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

These certifications cover AWS's infrastructure, data centers, and operational controls.

Veros leverages AWS's certified infrastructure while remaining fully responsible for application-level security, logical access control, encryption and data protection within the AWS environment.

3. Data Encryption

Veros encrypts customer data:

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

Encryption keys are managed through AWS Key Management Service (KMS) with strict access control and audit logging.

These encryption standards apply across production and non-production environments.

4. Access Control & Authentication

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

Key measures include:

- Unique user accounts
- Strong password requirements
- Optional or company-enforced Multi-Factor Authentication (MFA)
- Mandatory MFA for Veros staff accessing production systems
- Role-Based Access Control (RBAC)
- Logical tenant separation in a multi-tenant architecture
- No direct database access for users
- Controlled and logged production access for authorized personnel only

Administrative access rights are reviewed periodically and adjusted upon role changes.

5. Secure Software Development

Veros follows a secure software development lifecycle (SSDLC).

Key elements include:

- Source code hosted in GitHub with mandatory two-factor authentication
- Pull-request-based development workflow
- Mandatory peer review
- Automated testing before deployment
- Segregation between development and production environments
- Fully logged, API-driven deployment process
- No direct shell access to production servers

Security updates and dependency patches are monitored continuously and validated prior to release.

AI-assisted development tools are used only as productivity support. All outputs are reviewed and validated by Veros engineers before deployment.

6. AI Data Protection Standards

Where AI functionality is used within the Veros platform:

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

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

Veros' AI philosophy prioritizes transparency, explainability, and human oversight.

7. Monitoring & Logging

Veros leverages AWS-native monitoring and logging services, including:

- CloudTrail
- CloudWatch
- Application-level audit logging

Logging supports:

- Security monitoring
- Anomaly detection
- Operational diagnostics
- Full traceability of user actions

Sensitive data is not logged in plaintext.

Third-party access to raw logs is not provided in the standard multi-tenant environment. Incident summaries and relevant findings are provided where appropriate.

8. Incident Management

Veros maintains a formal Incident Response Policy covering the detection, containment, investigation, and remediation of security incidents.

Where a confirmed security incident affects customer data, affected customers are notified without undue delay and in any case within 24 hours of confirmed discovery.

If an incident involves personal data and qualifies as a personal data breach under the General Data Protection Regulation (GDPR), Veros applies additional procedures under its GDPR Data Breach Response Policy and fulfills its notification obligations in accordance with its role under applicable data protection law.

All incidents undergo documented investigation, root cause analysis, and implementation of corrective and preventive measures.

9. Business Continuity & Backup

Veros uses AWS-managed database backups with:

- Automated encryption
- Point-in-time recovery capability
- Regionally contained storage within the EU

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

10. Vendor & Subprocessor Management

Veros applies 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.

11. Contact

For security-related questions:

security@veros.ai