Security Whitepaper

Last updated: 03 March 2026

Organisation number: 936 578 195 | contact@opisense.com

1. INTRODUCTION

Opisense is an AI-powered business platform combining an intelligent workspace (Opispace), AI agents, and an integration and security layer (Opilogic) to help companies manage and automate their operations. This whitepaper describes the security architecture, practices, and compliance posture of the Opisense platform.

2. COMPLIANCE AND CERTIFICATIONS

Current status:

GDPR: Fully compliant. Data Processing Agreement available at opisense.com/legal.

EU AI Act: Aligned with transparency and human oversight requirements for AI systems.

ISO 27001:2022: Certification process initiated. Target completion: H2 2026.

SOC 2 Type II: Under evaluation. Timeline to be confirmed.

Opisense is registered with the Norwegian Data Protection Authority (Datatilsynet) and operates under Norwegian and EU data protection law.

2.1 Information security management

Opisense maintains a formal Information Security Management System (ISMS) in accordance with ISO 27001:2022. The ISMS policy is approved by management and reviewed annually. It establishes the framework for setting information security objectives, defines roles and responsibilities, and commits to continual improvement of the ISMS.

The ISMS encompasses asset management, including an information asset register and classification scheme covering all data processed through the platform. Assets are classified by confidentiality, integrity, and availability requirements, with appropriate controls applied to each classification level.

2.2 Physical security

As a cloud-native platform, Opisense relies on AWS for physical infrastructure security. AWS data centres maintain ISO 27001-certified physical security controls including multi-layer perimeter security, biometric access, 24/7 surveillance, and environmental controls.

For Opisense office premises, the following controls are in place: restricted physical access to office areas with key-card or equivalent access control, clean-desk policy for all staff handling customer or sensitive data, encrypted endpoint devices (laptops and mobile devices) with remote wipe capability, and secure disposal of physical media containing data.

3. INFRASTRUCTURE AND HOSTING

The platform is hosted on Amazon Web Services (AWS) in the Frankfurt (eu-central-1) region. Application delivery is handled through Vercel's edge network. Backend data infrastructure runs on Convex. AWS maintains ISO 27001, SOC 2, and numerous other certifications. Opisense leverages AWS security features including VPC isolation, security groups, and automated patching.

4. DATA ENCRYPTION

In transit: All data transmitted between users, the platform, and integrated services is encrypted using TLS 1.3.

At rest: All stored data is encrypted using AES-256 encryption.

Key management: Encryption keys are managed through AWS Key Management Service (KMS) with automatic key rotation.

5. ACCESS CONTROL

Role-based access control (RBAC) is enforced across the platform.

Multi-factor authentication (MFA) is required for all administrative and Opisense staff accounts, and available for all platform user accounts. Customers are encouraged to enforce MFA for all users through their account settings.

Administrative access to production systems is restricted, logged, and reviewed.

Least-privilege principles are applied to all system and service accounts.

User authentication is managed through Clerk with session management and token-based access.

Platform activity is monitored through Axiom for security event detection and anomaly alerting. These mechanisms, combined with the expanded provider list, ensure comprehensive access management and security monitoring.

6. AI MODEL SECURITY

The platform integrates with third-party AI model providers through API connections with zero-data-retention configurations. The expanded provider list includes OpenAI, Anthropic, and other vetted AI service providers.

Customer data is not used to train third-party AI models.

AI model outputs are clearly identified as AI-generated within the platform.

The platform enforces content filtering and safety boundaries on AI interactions.

Voice processing, including speech-to-text and text-to-speech, is provided through Elevenlabs under zero-retention API terms.

7. APPLICATION SECURITY

Secure development lifecycle (SDLC) practices are followed.

Code reviews are required for all production changes.

Dependency scanning is performed to identify known vulnerabilities.

Web application firewall (WAF) protects against common attack vectors.

8. RISK MANAGEMENT

Opisense maintains a risk register that is reviewed quarterly.

Risk assessments are conducted for new features, integrations, and sub-processors.

Data Protection Impact Assessments (DPIAs) are performed where required by GDPR.

9. OPERATIONS SECURITY

Logging and monitoring: Platform activity is logged through Axiom and monitored for security events.

Incident response: Documented incident response procedures with defined escalation paths.

Backup and recovery: Regular automated backups with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 24 hours each.

Change management: All production changes follow documented approval processes.

10. PERSONNEL SECURITY

All Opisense employees are subject to background verification appropriate to their role.

Security awareness training is provided to all personnel.

Access is revoked immediately upon termination of employment.

11. SUB-PROCESSOR MANAGEMENT

The platform relies on a comprehensive list of sub-processors for infrastructure, AI processing, authentication, payments, integrations, email delivery, and observability. This expanded provider list ensures service coverage and redundancy.

All sub-processors are subject to security assessment before engagement.

Sub-processor agreements include data protection and security requirements, including Standard Contractual Clauses for transfers outside the EU/EEA.

A current list of sub-processors is maintained at opisense.com/subprocessors.

Customers receive 30 days' notice before new sub-processors are engaged.

Transfer impact assessments are conducted for each sub-processor and reviewed when material changes occur.

12. BUSINESS CONTINUITY

Opisense maintains business continuity and disaster recovery plans.

Recovery objectives: RTO 24 hours, RPO 24 hours.

Plans are reviewed and tested annually.

13. FREQUENTLY ASKED QUESTIONS

Q: Where is my data stored?

A: Customer data is stored in AWS Frankfurt (eu-central-1) within the EU. Some processing occurs through US-based sub-processors under Standard Contractual Clauses.

Q: Is my data used to train AI models?

A: No. Customer data is never used to train AI models. Opisense enforces zero-data-retention policies with AI providers including OpenAI and Anthropic.

Q: Which AI providers does Opisense use?

A: The platform integrates with OpenAI and Anthropic for AI model inference, and Elevenlabs for voice processing. All operate under zero-data-retention API configurations.

Q: What happens to my data after contract termination?

A: Customer data is deleted on a tiered schedule following termination: Voice data is deleted within 7 days. Processed data (transcriptions, AI-generated output, metadata) is available for Customer export for 30 days and then deleted. Other personal data is deleted within 60 days. Data retained to comply with legal obligations (such as billing records under the Norwegian Bookkeeping Act) is retained as required by law. Written confirmation of deletion is provided within 14 days of each applicable deadline, as set out in the Data Processing Agreement.

Q: How do I report a security concern?

A: Contact security@opisense.com or your account representative.

Q: Can I request a penetration test report?

A: Yes. Contact security@opisense.com for the latest report summary.