Acceptable Use Policy

Last updated: 1 April 2026

1. INTRODUCTION

This Acceptable Use Policy (AUP) sets out the rules and restrictions that govern Customer and User access to and use of the Opisense platform. This policy applies in conjunction with the Master Services Agreement and Terms of Service and reflects Opisense's commitment to responsible AI deployment under the EU AI Act Article 5 and security obligations under the NIS2 Directive.

2. SCOPE

This AUP applies to all Customers and Users of the Opisense platform, regardless of subscription tier. Breach of this policy may result in suspension or termination of service.

3. PERMITTED USE

The Opisense platform is licensed for lawful, legitimate business purposes. Permitted uses include:

- Operational support and business automation
- Knowledge management and content creation
- Meeting analysis and transcription
- Analytics and business intelligence
- Employee development and training
- Customer support and engagement
- Workflow automation aligned with applicable law

All use must comply with Norwegian law, EU law (including GDPR and the EU AI Act), and the laws of jurisdictions where the Customer operates.

4. GENERAL PROHIBITED USES

The following uses are strictly prohibited:

4.1 ILLEGAL ACTIVITY

- Use for unlawful purposes or in breach of law
- Circumventing or attempting to bypass security measures
- Unauthorized access to accounts, data, or systems
- Transmission of malicious code, viruses, or worms
- Interference with platform availability or functionality

4.2 INTELLECTUAL PROPERTY VIOLATIONS

- Infringement of third-party intellectual property rights
- Unauthorized reproduction or distribution of copyrighted content
- Violation of trademark or patent rights
- Trade secret misappropriation

4.3 DATA PROTECTION VIOLATIONS

- Processing personal data without legal basis or consent
- Collection of data beyond the scope of legitimate business purposes
- Unauthorized transmission of confidential or sensitive data
- Circumvention of data protection controls

All data processing must comply with GDPR, the Norwegian Personal Data Act, and applicable data protection law.

4.4 MISUSE OF PLATFORM RESOURCES

- Resale or redistribution of platform access without authorization
- Excessive consumption of resources that impacts other users
- Use of platform for unauthorized benchmarking or reverse engineering
- Automation that violates pricing terms or exceeds usage limits
- Mining or scraping of data from other users' content

5. AI-SPECIFIC RESTRICTIONS

The Opisense platform incorporates AI systems governed by the EU AI Act. The following uses are prohibited to ensure responsible AI deployment and safeguard against harmful outcomes:

5.1 PROHIBITED AI USE CASES

- Social credit systems or discriminatory profiling
- Mass surveillance of individuals
- Emotion recognition for employment, law enforcement, or immigration decisions
- Targeted manipulation of vulnerable groups (minors, disabled persons)
- Use in law enforcement or criminal justice without appropriate safeguards
- Automated decision-making in legal, medical, or safety-critical contexts without human review

5.2 HIGH-RISK AI ACTIVITIES

Use of AI for high-risk purposes (biometric identification, educational decisions, employment, immigration, law enforcement) requires explicit written authorization from Opisense and documented human oversight protocols.

- Compliance with EU AI Act Article 5 requirements
- Implementation of explainability and human oversight
- Regular testing for bias and fairness
- Documentation of automated decision logic

5.3 AI OUTPUT RESPONSIBILITY

Customers acknowledge and accept responsibility for:

- Validating AI-generated content before use in critical decisions
- Implementing appropriate human oversight and review
- Not relying solely on AI output for legal, medical, or safety-critical decisions
- Monitoring for biased, unfair, or inaccurate outcomes
- Documenting AI system decisions as required by law

6. SECURITY AND COMPLIANCE RESTRICTIONS

6.1 SECURITY ABUSE

- Denial-of-service (DoS) attacks or attempts
- Vulnerability exploitation for unauthorized gain
- Network intrusion or scanning
- Social engineering or phishing

6.2 NIS2 DIRECTIVE COMPLIANCE

Customers must not use the platform in ways that compromise supply chain security or critical infrastructure protection requirements under the NIS2 Directive. Prohibited activities include:

- Introduction of malware or backdoors
- Compromise of authentication or encryption mechanisms
- Unauthorized data exfiltration
- Disruption of incident response or security logging

7. CONTENT RESTRICTIONS

Customers and Users shall not submit to the platform:

- Hate speech or discriminatory content
- Sexually explicit or abusive material
- Violence or glorification of violence
- Child exploitation material
- Threats or harassment
- Misinformation intended to cause harm
- Content that violates third-party rights

8. CONSEQUENCES OF VIOLATION

8.1 SUSPENSION AND TERMINATION

Opisense may, without liability:

- Suspend access immediately for security threats or illegal activity
- Terminate service for material or repeated violations
- Disable specific features if use violates this policy
- Report illegal activity to law enforcement

8.2 DATA HANDLING UPON VIOLATION

Upon suspension or termination for policy violation:

- Voice data is deleted after 7 days
- Customers may export non-violative processed data for 30 days
- Data used to investigate violations may be retained as required by law

9. MONITORING AND ENFORCEMENT

Opisense monitors platform use to detect and prevent violations. Monitoring methods include:

- Automated detection of malware, DoS patterns, and known attacks
- Analysis of usage patterns for suspicious activity
- Investigation of user reports and complaints
- Security audits and compliance reviews

Opisense does not proactively monitor the content of communications but may analyze content when investigating reported violations or security threats.

Acceptable Use Policy

Last updated: 1 April 2026

10. CUSTOMER RESPONSIBILITY

Customers are responsible for:

- Ensuring Users comply with this policy
- Monitoring User activity and conducting audits
- Immediately reporting violations to contact@opisense.com
- Implementing controls to prevent misuse
- Maintaining confidentiality of authentication credentials

11. DATA PROTECTION ALIGNMENT

This policy aligns with data protection principles under GDPR, the Norwegian Personal Data Act, and the EU AI Act. Processing must have a lawful basis, be necessary for the declared purpose, and implement appropriate safeguards.

12. CHANGES TO THIS POLICY

Opisense may update this policy with 30 days' written notice. Material changes grant Customers the right to terminate without penalty within 10 business days of the change taking effect.

13. REPORTING VIOLATIONS

To report a suspected violation:

- Email: contact@opisense.com
- Include details of the violation and any supporting evidence
- Opisense will investigate and respond within 10 business days

14. CONTACT INFORMATION

- Email: contact@opisense.com
- Website: opisense.com
- Organisation number: 936 578 195