ANANTIS

Anantis Terms and Conditions

End User License Agreement (EULA)

Last updated: July 12, 2026

1. Introduction

By accessing, installing, or using the **Anantis TrapEye Deception Platform**, you agree to be bound by this Agreement between **Anantis** ("Anantis", "We", "Our") and you ("Customer", "You").

We believe in being clear and concise about where our responsibility ends and yours begins. If anything is unclear, please contact us at .

---

2. Interpretation and Definitions

2.1 Definitions

- **Agreement**: These Terms, together with any applicable Order Forms or Statements of Work (SOW).
- **Order Form**: A document executed by both parties specifying the Services purchased, subscription term, pricing, and any commercial terms.
- **Authorized User**: People in your organization permitted to access the Platform.
- **Competitor**: Any entity developing products similar to TrapEye (Deception technology or Threat Intel).
- **Traps**: Virtual or physical simulation assets (servers, IoT, etc.) deployed to deceive attackers.
- **Lures**: Fictive data or credentials placed on real assets to redirect attackers toward Traps.
- **Platform / Service**: The TrapEye Deception Platform, including the Console, Traps, and APIs.
- **Threat Data**: Technical data related to malicious activity detected (IPs, TTPs, malware), excluding your business data.

---

3. Access & License Rights

3.1 License Grant

Subject to payment, Anantis grants you a non-exclusive, non-transferable license during your subscription to access the Console and deploy Traps for your internal security.

3.2 Evaluation License (POC)

During a trial or Proof of Concept, the Service is provided "as is" without any warranty. Traps deployed during a trial should not be used to protect critical production data unless specified.

3.3 Restrictions

To protect our technology, you agree not to:

- Allow any Anantis Competitor, or any individual acting on behalf of or affiliated with a Competitor, to access, evaluate, view, test, or otherwise use the Platform, whether directly or indirectly, without Anantis's prior written consent.
- Reverse engineer, decompile, or attempt to derive the source code of our Traps.
- Conduct benchmark tests or publish performance data without our written consent.
- Remove any proprietary notices or labels from the Service.

Any violation of this section shall constitute a material breach of this Agreement and may result in immediate termination of the Service. Anantis reserves the right to pursue any legal remedies available under applicable law, including injunctive relief and claims for financial damages.

---

4. Proprietary Rights

4.1 Ownership

Anantis and its licensors retain all rights, title, and interest in the TrapEye Platform. You obtain a license to use it, not ownership of the software itself.

4.2 Threat Intelligence & Feedback

- **Threat Data**: You grant Anantis the right to process aggregated and anonymized Threat Data for the purpose of improving the Service, developing security capabilities, and producing threat intelligence.
- **Feedback & Suggestions**: Any feedback, ideas, or suggestions you provide may be used by Anantis without restriction. You grant Anantis a worldwide, perpetual, royalty-free, sublicensable license to use, modify, and build upon such feedback.

---

5. Operations & Reliability

5.1 Maintenance & Downtime

We strive for constant availability, but brief downtime for maintenance is sometimes necessary. During these windows, Traps continue to log events locally and sync once the Console is back online.

5.2 Disaster Recovery

We maintain a disaster recovery plan. Our target recovery time (RTO) is 24 hours, and our target recovery point (RPO) is 24 hours. Infrastructure is fully version-controlled (GitOps) and can be restored from backup.

5.3 Incident Notification

In the event of a security incident with confirmed or potential impact on your data or services, Anantis will notify you as follows:

- **Initial notification:** within 4 hours of incident classification

- **Intermediate update:** within 72 hours of initial notification
- **Final report:** within 30 days of resolution, including root cause and remediation actions

For regulated financial entity customers subject to DORA (Regulation EU 2022/2554), Anantis provides all technical information necessary to fulfil your incident reporting obligations to your competent authority.

5.4 Security of Instructions

Anantis is authorized to act on any instruction received from an Authorized User's account. We are not liable for damages if an account is compromised, unless you notified us of the breach before we acted.

---

6. Customer Responsibilities & Risks

6.1 Deception Risks

Deception technology involves attracting attackers. By design, TrapEye appliances use isolated interfaces to prevent lateral movement. However, you remain responsible for your overall network security policy and ensuring the proper deployment of Traps within your authorized infrastructure.

6.2 High-Risk Activities

The Platform is **not designed for use in high-risk environments**, including but not limited to: nuclear facilities, aircraft systems, life-support equipment, or any scenario where failure could lead to death, injury, or severe property damage. Use in such environments is strictly at your own risk.

---

7. Fees and Payment

7.1 Payment Terms

Invoices are due within 30 days. Overdue amounts are subject to a late charge of 1.5% per month. Fees are non-refundable except as expressly provided in this Agreement or applicable Order Form.

7.2 Right to Audit

Anantis may, with reasonable notice, audit Customer's use of the Platform (e.g., number of deployed Traps) to verify compliance with the applicable subscription plan. If the audit reveals usage exceeding the purchased subscription level, Customer agrees to pay the applicable additional fees for the period during which such excess usage occurred and to upgrade to the appropriate subscription level going forward.

---

8. Data Protection & Privacy (GDPR)

8.1 Sovereignty & Residency

Customer Data is primarily hosted on **Exoscale infrastructure located in Geneva and Zurich, Switzerland**. Upon Customer request and subject to applicable commercial terms, Anantis may provide hosting options in other jurisdictions.

Switzerland benefits from a GDPR adequacy decision by the European Commission, ensuring an adequate level of data protection. Customer Data is not hosted outside the selected hosting jurisdiction, except as required for support, maintenance, or legal obligations.

Anantis operates as a Data Processor, and processing activities are strictly limited to the performance of the Service. A Data Processing Agreement (DPA) is available upon request and forms part of this Agreement.

8.2 Data Minimization & Retention

We only collect the technical data strictly necessary for threat detection. You retain full ownership of your data, including the right to export or request its permanent deletion at any time.

Personal data (platform user email addresses) is retained for the duration of the contract and deleted within 30 days of termination. The default retention period is 1 year after contract end, unless otherwise agreed in writing. Detection data (Trap events, attacker IPs, alert context) is retained for the duration of the contract and deleted upon termination.

8.3 Security Measures

Anantis implements industry-standard administrative, technical and organizational safeguards to protect Customer data, including:

- Encryption in transit (TLS 1.2+) and encryption at rest
- Multi-factor authentication (MFA) for administrative access
- Role-Based Access Control (RBAC)
- Infrastructure-as-Code and GitOps for reproducible, version-controlled deployments
- Daily encrypted backups
- Security logging and monitoring of the Platform

---

9. Confidentiality

9.1 Definition

Confidential Information includes all non-public information disclosed by one party to the other, including trade secrets, product roadmaps, security incident details, and network architecture.

9.2 Obligations

Each party agrees to protect the other's Confidential Information with the same degree of care as its own. This obligation remains in effect during the Agreement and for five (5) years after its termination.

---

10. Acceptable & Lawful Use

10.1 Authorized Perimeter

You may only deploy Traps and Lures on systems and networks that you own or are legally authorized to monitor.

10.2 Prohibited Use

You shall not use the Service to conduct offensive operations against third parties, engage in illegal surveillance, or interfere with the stability of third-party infrastructure. You agree to indemnify Anantis against any legal action resulting from use outside of your authorized perimeter.

---

11. Support & Service Levels

11.1 Support Channels

Technical support is provided via email at **support@anantis.io**.

11.2 Support Hours

Support is provided during standard business hours (Monday to Friday, 9:00 AM to 6:00 PM CET).

11.3 Support Response Targets

Depending on the severity of the reported issue, Anantis targets the following initial response times during Business Hours.

These targets refer only to the initial acknowledgment and assessment of the request and do not constitute guaranteed resolution times.

Priority	Description	Initial Response Target
P1: Critical	Service unavailable, Console inaccessible, or Traps unable to send events	4 business hours
P2: High	Significant degradation or major functionality unavailable without workaround	8 business hours
P3: Normal	Functional issue, configuration assistance, deployment assistance, or integration question	2 business days
P4: Low	Documentation questions, feature requests, or general inquiries	5 business days

11.4 Platform Availability

Anantis targets a monthly Service Availability of **99.8%** for the Console and APIs, calculated as follows:

```
Availability = ((Total Minutes − Unavailable Minutes) / Total Minutes) × 100
```

Availability excludes:

- Scheduled maintenance announced at least 48 hours in advance;
- Emergency maintenance required to preserve the security or integrity of the Service;
- Force Majeure Events (Section 13);
- Unavailability caused by Customer's own network, Internet connectivity, or third-party infrastructure outside Anantis's reasonable control.

Current and historical Service availability is published for information purposes at **status.anantis.io**. This status page is provided for transparency and does not itself constitute the contractual measurement of Availability, which is determined solely under this Section 11.4.

11.5 Service Credits

If monthly Availability falls below the target set out in Section 11.4, Customer may request the following service credits, applied against the fees for the affected month only:

Monthly Availability	Service Credit
99.0% – 99.79%	5%
98.0% – 98.99%	10%
Below 98.0%	25%

Service Credits are Customer's sole and exclusive remedy for any failure to meet the Availability target. To be eligible for a Service Credit, a request must be submitted in writing to support@anantis.io within thirty (30) days after the end of the affected month. Failure to submit such a request within this period shall result in the forfeiture of the right to claim a Service Credit for that month.

---

12. Warranties, Liability & Insurance

12.1 Limited Warranty

If the Platform materially fails to perform as described in the Documentation, Anantis will use commercially reasonable efforts to correct the issue. If Anantis is unable to do so within a reasonable period, Customer may be eligible for a pro-rata refund of the affected subscription fees.

12.2 Third-Party Software & Open Source

The Platform may include third-party software or open-source components. Such components are subject to their respective licenses. Anantis provides the Platform "as is" with respect to these components and makes no additional warranty beyond what the third-party licenses provide.

12.3 Disclaimer

Except for the express warranties above, the service is provided "as is". Anantis does not warrant that TrapEye will detect all threats, prevent all intrusions or be error-free. It is a detection tool, not a guarantee of absolute security.

12.4 Limitation of Liability

To the maximum extent permitted by law, Anantis's total liability for any claim will not exceed the total fees you paid us in the 12 months preceding the incident. Neither party is liable for any indirect, incidental, special, consequential, or punitive damages, including loss of profits, data, or business interruption.

12.5 Insurance & Waiver

You agree to maintain your own cyber-liability insurance. You agree to look solely to your insurer for recovery of any loss and waive any claims against Anantis.

---

13. Force Majeure Events

Neither party shall be liable for any failure or delay in performance (except for payment obligations) due to causes beyond its reasonable control, including but not limited to acts of God, war, terrorism, pandemic, riots, embargoes, fire, floods, accidents, strikes, or failure of the public internet or third-party cloud providers.

---

14. Term and Termination

14.1 Term & Termination

Subscription terms are specified in the applicable Order Form. Unless otherwise stated, subscriptions automatically renew for successive periods and may be terminated with thirty (30) days' notice before renewal.

If you breach a material provision, we may terminate the service immediately.

14.2 Effect of Termination

Upon termination, you must stop using the Platform and remove all Lures and Traps from your network. Any physical hardware provided by Anantis must be returned within 14 days. Any unpaid fees become due immediately.

---

15. General Provisions

15.1 Statute of Limitations

Any legal claim related to this Service must be filed within 12 months after the incident occurred, or it will be forever barred.

15.2 Injunctive Relief

If you violate our intellectual property or usage restrictions, Anantis has the right to seek an immediate court order to stop the violation.

15.3 Governing Law & Jurisdiction

This Agreement shall be governed by the laws of Switzerland.

Any dispute arising out of or in connection with this Agreement shall be submitted to the exclusive jurisdiction of the competent courts of Geneva, Switzerland.

15.4 Assignment

Neither party may assign or transfer this Agreement, in whole or in part, without the other party's prior written consent, except that either party may assign this Agreement without consent in connection with a merger, acquisition, or sale of substantially all of its assets.

15.5 Severability

If any provision of this Agreement is held to be invalid or unenforceable, that provision shall be limited or eliminated to the minimum extent necessary, and the remaining provisions shall remain in full force and effect.

15.6 Order of Precedence

If there is any conflict between these Terms and an executed Order Form, the Order Form shall prevail solely with respect to that conflict.

15.7 Entire Agreement

This Agreement, including these Terms and any executed Order Forms, constitutes the entire agreement between the parties regarding the Service and supersedes all prior agreements, communications, or understandings.

15.8 Modifications to Terms

Anantis reserves the right to modify these Terms at any time. Changes become effective immediately upon being posted on our website. Your continued use of the Service following such changes constitutes your acceptance of the revised Terms. If you do not agree to the updated Terms, your sole remedy is to stop using the Service.

15.9 Contact Us

For any questions regarding these Terms, contact us at: **support@anantis.io**