

Ciptor Sweden Terms of Service

Last Updated: July 20, 2026
Effective Date: July 20, 2026

1. Introduction and Acceptance

1.1 Acceptance of Terms

These Terms of Service ("Terms") constitute a legally binding agreement between you ("User," "you," or "your") and **Ciptor Sweden AB** (reg. no. **556819-5985**) ("we," "us," "our," or "Company").

Ciptor Sweden AB is part of the international **Ciptor corporate group**, which includes, but is not limited to:

- **Ciptor America Inc** (Tax ID: 83-2388188)
- **Ciptor ITSAFE Canada**
- **Ciptor Finland**
- **Ciptor Benelux B.V.B.A**
- **Ciptor Turkey,**
- **Ciptor Thailand,** and other regional Ciptor group entities.

These Terms govern your access to and use of the Ciptor ecosystem and platforms (collectively, the "**Platform**"), including **Ciptor Shield, Ciptor Cyber Security Operations Framework (CSOF), Ciptor Cybersecurity Assessments**, hardware-backed identity management services, related software, web applications, APIs, features, and content (collectively, the "**Services**").

Ciptor Sweden AB may engage other entities within the Ciptor corporate group or certified third-party technology partners to provide certain parts of the Services. You may therefore receive communications, support, or services from any group entity, but your primary contractual relationship remains with Ciptor Sweden AB.

You must read and expressly accept these Terms before creating an account or using the Services. During the registration process, you will be required to confirm that you have read, understood, and agree to be bound by these Terms by checking the acceptance box or signing a service agreement.

If you do not agree to these Terms, you may not create an account or use the Services. By accepting these Terms, you confirm that you accept them on your own behalf and, where applicable, on behalf of the organization you represent.

1.2 Eligibility

You must be at least **18 years old** and have full legal capacity to enter into binding agreements to use our Services. By using the Services, you represent and warrant that you meet these requirements.

The Services are designed for professional and enterprise use and are not intended for individuals under 18 years of age. We do not knowingly collect personal data from minors. If we become aware that a user is under 18, we will promptly terminate their account and delete their personal data, except where retention is required by law. If you believe a minor has created an account, please contact us immediately at **info@ciptor.com**.

For Business Users: By accepting these Terms, you confirm and warrant that you have full legal authority to bind your company or organization to these Terms.

1.3 Changes to Terms

We may update these Terms from time to time to reflect regulatory changes (such as updates to EU NIS2, DORA, or GDPR enforcement), platform enhancements, or new operational practices.

- **Material Changes:** Notified at least **30 days in advance** via email or prominent platform notification.
- **Minor Updates:** Take effect immediately upon posting to our website (www.ciptor.com).
- **Urgent Changes:** Changes required by law, regulatory mandates, or urgent security reasons may take effect immediately.

Continued use of the Services after the effective date of an updated version constitutes acceptance of the revised Terms. If you do not agree, you must immediately stop using the Services and close your account.

2. Description of Services

2.1 Platform Overview

Ciptor provides modular cybersecurity solutions designed to build total organizational cyber resilience across identity, infrastructure, and intelligence, including:

- **Ciptor Cybersecurity Assessments:** Interactive diagnostic tools, automated gap analysis, NIS2/DORA posture evaluation, and actionable remediation roadmaps.
- **Ciptor Shield:** Phishing-resistant, hardware-backed identity access management (IAM) utilizing passwordless FIDO2 protocols, liveness proofing, and credential reset protection.
- **Ciptor CSOF (Cyber Security Operations Framework):** AI-powered threat detection, automated incident response, identity risk mitigation, and dark web intelligence monitoring.
- **Reporting & Integrations:** Interactive dashboards, automated export functionalities (e.g., PDF/JSON), and integrations with verified hardware keys and enterprise IT environments.

2.2 Service Models and Tiers

Services may be offered under various subscription models, including freemium tiers, trial periods, or custom enterprise licenses:

- **Free & Trial Tiers:** Granted for evaluation purposes with limited features or report generations as indicated on the Platform. We reserve the right to modify, adjust, or discontinue free-tier limitations prospectively at our discretion.
- **Enterprise & Paid Tiers:** Specific pricing, license limits, service level targets (SLAs), and features for paid tiers are set out in separate order forms, statements of work, or billing pages on the Platform.

2.3 AI-Powered Features and Limitations

The Services leverage advanced artificial intelligence (AI) models and machine learning frameworks (e.g., automated threat analysis, risk scoring, and report generation). In accordance with applicable AI transparency standards (such as the EU AI Act):

- **Informational Purpose Only:** AI-generated outputs, threat scores, and recommendations are provided for informational and preliminary guidance purposes. They do **not** constitute formal legal, financial, or certified security audit advice.

- **Verification Required:** While designed to offer high precision, AI outputs may occasionally contain inaccuracies or incomplete context. You remain solely responsible for independently verifying recommendations and consulting qualified internal or external cybersecurity professionals prior to taking critical infrastructure actions.

2.4 Service Changes and Availability

We continuously refine our platform to adapt to emerging cyber threats. We reserve the right to modify, update, or deprecate features or components of the Services. While Ciptor strives to provide high availability and zero-trust uptime, we do not guarantee uninterrupted, latency-free, or error-free operation. Scheduled maintenance or emergency security patching may result in brief service interruptions.

3. User Accounts and Authentication

3.1 Account Creation & Passwordless Authentication

To access the Platform, users must create an account using verified authentication mechanisms (e.g., enterprise SSO, magic links, or FIDO2 security keys). You must provide accurate, complete, and current information, including a valid business email address. Maintaining multiple accounts for fraudulent or unauthorized purposes is strictly prohibited.

3.2 Account Security & Credentials

You are responsible for maintaining the confidentiality and control of your authentication devices, security keys, and access tokens. You must immediately notify Ciptor at security@ciptor.com or info@ciptor.com upon suspecting any unauthorized access, compromised device, or security breach. Ciptor is not liable for losses caused by compromised user-side credentials.

3.3 Account Suspension and Termination

We reserve the right to suspend or terminate access to the Platform with or without prior notice if:

- You breach any provision of these Terms or the Acceptable Use Policy.
- Your account poses an active security threat to Ciptor, our partners, or other users.
- Required by law enforcement or regulatory authorities.
- Your account remains inactive for an extended period (subject to advance warning).

You may request account deletion at any time via the account settings panel or by contacting support. Personal data will be deleted or anonymized in accordance with our Privacy Policy and applicable data protection laws.

4. Data Security and Encryption

4.1 Encryption and Architectural Safeguards

Ciptor implements technical and organizational measures designed to protect sensitive cybersecurity data, including:

- **In Transit:** All data transmitted between your endpoints and the Platform is encrypted using modern TLS protocols.
- **At Rest:** Platform data is encrypted at rest using industry-standard AES-256 encryption.
- **Application-Level Encryption:** Sensitive user inputs, assessment responses, and credential tokens utilize application-level encryption with key segregation

(e.g., AES-256-GCM), ensuring data privacy even if underlying storage components are compromised.

- **Certified Hardware:** Hardware components deployed via Ciptor Shield adhere to rigorous independent certifications (e.g., FIDO2, Common Criteria EAL5+/EAL6+, FIPS 140-3).

4.2 Key Management

Cryptographic keys are managed using key versioning protocols and segregated key management infrastructure. Users do not have direct access to internal master cryptographic keys.

4.3 Security Incident Notification

In the event of a confirmed data breach impacting your personal or organizational data:

1. **Regulatory Reporting:** We will notify the **Swedish Authority for Privacy Protection (IMY)** within **72 hours** of becoming aware of the breach, where required under GDPR, as well as relevant authorities under NIS2/DORA mandates.
2. **User Notification:** We will notify affected users without undue delay if the incident poses a high risk to their rights, freedoms, or network security.

5. Privacy and Data Protection

5.1 Privacy Policy

Our processing of personal data is fully detailed in our **Privacy Policy** (available at https://ciptor.com/content/files/documents/privacy_policy.pdf). By using the Services, you acknowledge the collection, use, and processing of personal data as described therein.

5.2 Regulatory Compliance

For users in the European Economic Area (EEA), Ciptor Sweden AB complies with the **GDPR**. For users in the US or other international regions, we comply with relevant applicable frameworks (such as the Florida Digital Bill of Rights (FDBR) and CCPA). You retain full rights to access, rectify, restrict, or request erasure of your personal data.

5.3 Cookies and Tracking

We utilize essential cookies required for basic platform operation, authentication, and security. Non-essential analytical cookies require your express opt-in consent, which you can modify at any time in our cookie preference center.

6. Intellectual Property Rights

6.1 Platform Ownership

All right, title, and interest in and to the Platform and Services—including all software code, proprietary security frameworks, algorithms, assessment logic, trade secrets, logos, and trademarks (including "Ciptor", "Ciptor Shield", and "Ciptor CSOF")—are and shall remain the exclusive property of **Ciptor Sweden AB**, its group entities, or its licensors.

6.2 Limited User License

Subject to full compliance with these Terms, Ciptor grants you a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the Services solely for your **internal business security purposes**.

6.3 Usage Restrictions

You shall **not**, directly or indirectly:

- Copy, modify, decompile, reverse-engineer, disassemble, or extract source code or underlying logic from the Platform or reports.
- Remove, obscure, or alter any copyright, trademark, or proprietary rights notices.
- Use automated scrapers, bots, or crawlers to access or extract data from the Platform without prior written consent.
- Resell, sublicense, lease, time-share, or commercialize the Services or AI-generated output to third parties without an authorized partner agreement.
- Use the Platform to develop competing security analysis tools, models, or frameworks.
- Interference with or disruption of the integrity, stability, or security of the Platform.

6.4 User Data and Generated Reports

Data Type	Ownership & License Terms
Input Data (e.g., network configs, assessment answers, logs)	You retain full ownership. You grant Ciptor a worldwide, royalty-free license to store, process, and transmit this data solely to provide, support, and secure the Services for you.
Anonymized & Aggregated Data	Ciptor may extract, aggregate, and anonymize technical metadata to improve threat intelligence models, refine benchmarking, and optimize AI models. This data cannot reasonably identify you or your organization.
Generated Reports & Downloads	Reports generated by the Platform are licensed to you for internal business security, compliance, and auditing purposes . You may share them with your internal teams, external auditors, and regulators. You may not commercialize or resell these reports.

6.5 Feedback

If you provide Ciptor with ideas, feature requests, or improvement suggestions ("Feedback"), you grant us an irrevocable, perpetual, worldwide, royalty-free license to implement and exploit such Feedback without restriction or obligation to compensate you.

7. Acceptable Use Policy

7.1 Permitted Use

The Services must be used exclusively for lawful, internal cybersecurity risk assessment, threat detection, identity protection, and regulatory compliance management.

7.2 Prohibited Actions

You agree **not** to:

- Conduct unauthorized security testing, penetration testing, scanning, or probing against Ciptor's systems or third-party environments without explicit authorization.
- Intercept, manipulate, or forge network packets or authentication tokens.
- Upload or distribute malicious code, ransomware, logic bombs, or spyware.
- Impersonate any entity or misrepresent your organization's affiliation.
- Use the Services in violation of international cybercrime laws, data privacy acts, or trade controls.

Violation of these rules may lead to immediate account termination and reporting to competent legal authorities.

8. Fees, Payment, and Subscription

8.1 Commercial Terms

Access to paid features, enterprise keys, or custom CSOF modules requires payment of fees set forth in an Order Form, Statement of Work, or electronic checkout agreement.

8.2 Billing and Taxes

All fees are quoted exclusive of Value Added Tax (VAT), sales tax, or other applicable governmental levies, which will be calculated and added at checkout/invoicing based on your corporate tax jurisdiction.

8.3 Non-Refundability

Except where expressly mandated by applicable mandatory law or written agreement, paid fees are non-refundable once the service period has commenced or digital reports have been generated.

9. Communications and Notifications

To maintain system integrity and service delivery, Ciptor will send necessary administrative and technical communications, including:

- Security alerts, liveness verification prompts, and authentication notifications.
- System status updates, billing receipts, and legal term modifications.

Official communications may originate from official Ciptor group domains, including: @ciptor.com, @ciptoritsafe.com, or regional subgroup domains.

10. Third-Party Integrations and Dependencies

10.1 External Links & Integrations

The Platform may integrate with or link to third-party hardware, cloud infrastructure, or software partners (e.g., IBM, NVIDIA, Feitian, YubiKey, Neowave, Microsoft). Third-party services are subject to their respective terms and conditions.

10.2 Service Dependencies

While Ciptor selects world-class enterprise vendors, Ciptor is not liable for disruptions, service outages, or data availability failures caused directly by third-party cloud hosting providers or hardware supply chain interruptions beyond Ciptor's reasonable operational control.

11. Disclaimers and Limitations of Liability

"AS IS" DISCLAIMER: THE SERVICES AND PLATFORM ARE PROVIDED ON AN **"AS IS"** AND **"AS AVAILABLE"** BASIS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, CIPTOR SWEDEN AB DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, TITLE, AND NON-INFRINGEMENT.

- **No Guarantee of Absolute Security:** Cyber threat landscapes evolve rapidly. While Ciptor implements certified, state-of-the-art protections, no security framework can guarantee absolute immunity against zero-day exploits, state-sponsored cyberattacks, or catastrophic internal user errors.
- **Limitation of Indirect Damages:** To the fullest extent permitted by Swedish law, Ciptor Sweden AB, its officers, directors, employees, and group affiliates shall not be liable for any indirect, incidental, punitive, special, or consequential damages (including loss of profit, data breach recovery costs, business interruption, or operational downtime).
- **Cap on Liability:** In any event, Ciptor's total aggregate liability arising out of or related to these Terms or the Services shall be capped at the total amount actually paid by you to Ciptor Sweden AB for the specific Service in the **twelve (12) months** preceding the event giving rise to the claim (or **SEK 1,000** for free-tier usage).

12. Indemnification

You agree to defend, indemnify, and hold harmless **Ciptor Sweden AB**, its parent, subsidiaries, affiliates, officers, directors, employees, and agents from and against any third-party claims, liabilities, losses, damages, or costs (including reasonable legal fees) arising from:

1. Your breach of these Terms or the Acceptable Use Policy.
2. Unlawful or unauthorized data submitted by your organization to the Platform.
3. Your reliance on AI assessment reports as the sole legal or operational basis for compliance decisions without independent security verification.
4. Security breaches or failures occurring within your organization's internal infrastructure or endpoints that you claim resulted from improper implementation of platform recommendations.

13. Termination

13.1 User Termination

You may terminate your account at any time by accessing your account preferences or contacting **support@ciptor.com**.

13.2 Termination for Cause

Either party may terminate this agreement immediately if the other party materially breaches these Terms and fails to cure such breach within **14 days** of receiving written notice.

13.3 Termination Without Cause

Ciptor may terminate free accounts or non-binding subscriptions at any time with **30 days' written notice**.

13.4 Effect of Termination

Upon termination:

- **Access Rights:** All access rights and licenses granted to you shall immediately cease.
- **Data Export Window:** You will have **30 days** from the termination date to export your data and assessment reports.
- **Data Deletion:** Following the 30-day window, your personal data and assessment inputs will be deleted or anonymized, save for data retained under mandatory statutory retention periods (e.g., Swedish accounting regulations requiring 7-year records retention).

14. Dispute Resolution and Governing Law

14.1 Governing Law

These Terms, and any dispute or claim arising out of or in connection with them, shall be governed by and construed in accordance with the **substantive laws of Sweden**, excluding its conflict of law principles.

14.2 Jurisdiction

Any legal suit, action, or proceeding arising out of or related to these Terms or the Services shall be brought exclusively before the **Gothenburg District Court (Göteborgs tingsrätt)** as the court of first instance.

14.3 Informal Resolution

Before initiating formal litigation, the parties agree to make a good-faith attempt to resolve any dispute informally by submitting written notification to **info@ciptor.com**.

15. Export Controls and Sanctions

The Services, software, and certified hardware deployment models may be subject to international export control, dual-use regulations, and trade sanction laws (including those of Sweden, the European Union, and the United States). You agree not to access, export, re-export, or transfer any portion of the Services in violation of applicable sanction laws or to prohibited destinations/entities.

16. Accessibility

Ciptor is committed to digital accessibility across our web interfaces and software platforms. If you encounter accessibility barriers or require information in alternative formats, please contact us at **info@ciptor.com**.

17. Miscellaneous

- **Entire Agreement:** These Terms, alongside the Privacy Policy and any executed Order Forms, constitute the entire agreement between you and Ciptor Sweden AB regarding the Services.
- **Severability:** If any provision of these Terms is held invalid or unenforceable, the remaining provisions will continue in full force and effect.
- **No Waiver:** Ciptor's failure to enforce any right or provision shall not constitute a waiver of future enforcement.
- **Assignment:** You may not assign or transfer these Terms without Ciptor's prior written consent. Ciptor may assign its rights and obligations to group entities or successors in interest without restriction.
- **Force Majeure:** Ciptor shall not be liable for failure or delay in performance caused by circumstances beyond its reasonable control, including natural

disasters, acts of war, terrorism, cyber warfare, global internet backbone failures, pandemic restrictions, strikes, or governmental emergency mandates.

18. Contact Information

For questions, formal legal notices, or administrative inquiries regarding these Terms of Service, please contact:

Ciptor Sweden AB

- **Registration No:** 556819-5985
- **Address:** Kungsporten 4A, 427 50 Billdal, Sweden
- **General Email:** info@ciptor.com
- **Privacy & Security Email:** privacy@ciptor.com
- **Website:** www.ciptor.com