

# UNIBEAM CLOUD AUTHENTICATION SERVICES

## END USER LICENSE AGREEMENT

*Last Updated: May 2026 | AWS Marketplace Edition*

### AWS Marketplace Notice

**THIS AGREEMENT IS OFFERED BY UNIBEAM ("UNIBEAM", "SELLER") ON THE AWS MARKETPLACE, OPERATED BY AMAZON WEB SERVICES, INC. ("AWS"). BY SUBSCRIBING TO OR USING THE SERVICES VIA AWS MARKETPLACE, CUSTOMER AGREES TO BOTH THIS AGREEMENT AND THE AWS CUSTOMER AGREEMENT OR OTHER AGREEMENT WITH AWS GOVERNING CUSTOMER'S USE OF AWS SERVICES.**

In the event of any conflict between this Agreement and the AWS Customer Agreement with respect to the Services provided by Unibeam, this Agreement shall govern. AWS is not a party to this Agreement and has no obligations, warranties, or liability of any kind under this Agreement. All billing and payment for the Services are handled through AWS Marketplace in accordance with AWS billing terms.

### 1. Services

Unibeam provides cloud-based authentication, SIM/eSIM-based identity assurance, device authentication, consent validation, fraud mitigation, and related security services ("Services").

The Services may include:

- SIM/eSIM-based authentication
- Device assurance
- Silent authentication
- Consent and approval workflows
- Identity verification signals
- APIs and SDKs
- Administrative portals
- Event logging and analytics
- Related telecom-integrated security services

Unibeam may update, improve, or modify the Services from time to time. Material changes to functionality will be communicated via the AWS Marketplace listing or Seller's documentation portal.

## 2. License and Permitted Use

Subject to this Agreement, Unibeam grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right to access and use the Services solely for Customer's internal business or governmental operations.

Customer shall not:

- Reverse engineer or attempt to extract source code, applets, cryptographic material, protocols, or APIs
- Interfere with or disrupt the Services or infrastructure supporting the Services
- Use the Services for unlawful, fraudulent, or unauthorized purposes
- Resell or redistribute the Services unless expressly authorized in writing by Unibeam
- Perform unauthorized security testing or benchmarking
- Use the Services to circumvent any authentication, access control, or security mechanism

## 3. Authentication and Security Disclaimer

The Services provide an additional authentication and device assurance layer designed to reduce the risk of unauthorized access, impersonation, fraud, phishing, and account compromise.

Unibeam does not guarantee:

- Prevention of all fraud or cyber incidents
- Continuous or uninterrupted service availability
- Absolute identity verification
- Prevention of unauthorized access in all circumstances

Authentication decisions, access approvals, and authorization policies remain solely the responsibility of Customer.

## 4. Telecom and Device Dependencies

Certain Service capabilities may depend on mobile network availability, SIM/eSIM provisioning status, roaming availability, device compatibility, operating system behavior, and third-party telecom infrastructure.

Unibeam shall not be responsible for failures or degraded performance caused by third-party infrastructure, telecom operators, device manufacturers, cloud providers (including AWS), or internet disruptions.

## 5. Customer Responsibilities

Customer is responsible for:

- Maintaining the security of its systems, credentials, and integration configurations
- Configuring authorization and access policies appropriate for its environment
- Obtaining required user consents under applicable law prior to authentication events
- Complying with all applicable laws, regulations, and industry standards
- Ensuring lawful use of the Services

Customer shall immediately notify Unibeam of any suspected security incident involving the Services.

## 6. Privacy and Data Protection

Use of the Services is subject to the Unibeam Privacy Policy and applicable data protection laws, including but not limited to GDPR, CCPA, and applicable telecom privacy regulations.

The Services may process:

- Device identifiers
- SIM/eSIM identifiers
- Authentication events and transaction metadata
- IP addresses
- Telemetry and security-related metadata

Customer represents that it has all necessary legal rights, permissions, and user consents to provide data to Unibeam for processing, and that such processing is permitted under applicable law.

## 7. Security

Unibeam implements commercially reasonable technical and organizational measures designed to protect the confidentiality, integrity, and availability of the Services, including:

- Encryption in transit and at rest
- Access controls and authentication
- Logging and monitoring
- Segmentation and isolation controls
- Incident response procedures

## 8. Intellectual Property

All intellectual property rights in the Services, software, APIs, applets, documentation, trademarks, and related technology remain the exclusive property of Unibeam and its licensors. No ownership rights are transferred to Customer under this Agreement.

Customer acknowledges that Unibeam's confidential technical information, including but not limited to SIM/eSIM authentication protocols, cryptographic methods, and applet architecture, constitutes valuable trade secrets. Unauthorized disclosure or misappropriation of such trade secrets shall constitute a material breach of this Agreement, and Unibeam shall be entitled to seek injunctive relief and all other remedies available at law or in equity.

## 9. Confidentiality

Each party shall protect the confidential information of the other party using at least the same degree of care used to protect its own confidential information, but in no event less than reasonable care, and shall not disclose such information except as required for performance under this Agreement or by applicable law.

Confidential information shall not include information that: (a) is or becomes publicly available through no fault of the receiving party; (b) was rightfully known to the receiving party prior to disclosure; (c) is independently developed by the receiving party without use of or reference to the disclosing party's confidential information; or (d) is required to be disclosed by law, regulation, or court order, provided the receiving party provides prompt prior written notice to the disclosing party.

**THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 12 SHALL NOT APPLY TO BREACHES OF THIS SECTION 9.**

## 10. Service Availability

Unibeam will use commercially reasonable efforts to maintain service availability. Scheduled maintenance, upgrades, emergency maintenance, telecom outages, or force majeure events may result in temporary interruptions.

Unless separately agreed in a written Service Level Agreement ("SLA") between the parties or specified in the applicable AWS Marketplace listing, no specific uptime commitment applies. Customers requiring guaranteed uptime commitments should contact Unibeam at [support@unibeam.io](mailto:support@unibeam.io) to arrange an enterprise SLA.

## 11. Suspension

Unibeam may suspend access to the Services immediately if:

- Customer violates this Agreement
- Unibeam reasonably suspects fraud, abuse, or security risks associated with Customer's account
- Required by applicable law, regulation, or governmental authority
- AWS requires suspension pursuant to its marketplace policies

Unibeam will endeavor to provide reasonable notice prior to suspension unless the suspension is required immediately to protect the integrity or security of the Services or other customers.

## 12. Limitation of Liability

**TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW:**

- UNIBEAM SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF DATA, BUSINESS INTERRUPTION, OR CYBER INCIDENTS CAUSED BY THIRD PARTIES
- UNIBEAM'S AGGREGATE LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO UNIBEAM DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO THE CLAIM

**NOTWITHSTANDING THE FOREGOING, THE LIABILITY LIMITATIONS IN THIS SECTION SHALL NOT APPLY TO: (A) BREACHES OF SECTION 9 (CONFIDENTIALITY); (B) INFRINGEMENT OF EITHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (C) CUSTOMER'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 13; OR (D) DAMAGES ARISING FROM FRAUD, WILLFUL MISCONDUCT, OR GROSS NEGLIGENCE.**

## 13. Indemnification

Customer shall indemnify, defend, and hold harmless Unibeam and its officers, directors, employees, and agents from and against any claims, liabilities, damages, losses, and expenses (including reasonable legal fees) arising from:

- Customer's misuse of the Services or breach of this Agreement
- Customer's violation of applicable law or regulation
- Customer's unauthorized processing of personal data
- Customer's systems, configurations, or authorization decisions
- Customer's end users' use or misuse of the Services

## 14. Compliance and Export Controls

Customer shall comply with all applicable export control laws, sanctions regulations, telecom regulations, cybersecurity regulations, and privacy and data protection laws.

Customer shall not use the Services in violation of applicable sanctions or restricted party regulations, including but not limited to regulations administered by the U.S. Office of Foreign Assets Control (OFAC), the EU, or the State of Israel. Customer represents and warrants that it is not located in, or acting on behalf of any person or entity located in, a country subject to applicable sanctions.

## 15. Government and Regulated Usage

The Services may be used by governmental entities, financial institutions, healthcare organizations, and regulated industries, subject to Customer's independent compliance obligations. Customer remains solely responsible for regulatory approvals, retention obligations, audit requirements, and lawful authorization decisions specific to its industry and jurisdiction.

## 16. Term and Termination

This Agreement remains effective until terminated in accordance with its terms or until Customer's AWS Marketplace subscription is terminated or expires.

Either party may terminate this Agreement: (a) upon material breach not cured within thirty (30) days of written notice; or (b) immediately for unlawful use, security risks, or insolvency proceedings.

Upon termination, Customer shall cease all use of the Services. Sections 8, 9, 12, 13, and 17 shall survive termination of this Agreement.

## 17. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of Israel, without regard to its conflict of law principles.

Any disputes arising out of or relating to this Agreement shall be subject to the exclusive jurisdiction of the competent courts located in Tel Aviv, Israel. Each party irrevocably submits to the personal jurisdiction of such courts for this purpose.

Notwithstanding the foregoing, either party may seek injunctive or other equitable relief in any court of competent jurisdiction to prevent irreparable harm, including but not limited to unauthorized disclosure of confidential information or infringement of intellectual property rights.

## 18. General Provisions

This Agreement constitutes the entire agreement between the parties regarding the Services and supersedes all prior agreements, representations, and understandings relating to the subject matter herein. In the event of a conflict between this Agreement and any order form, purchase order, or other document, this Agreement shall govern unless expressly stated otherwise in a separately signed written agreement.

If any provision of this Agreement is found to be unenforceable, the remaining provisions shall continue in full force and effect. No waiver of any provision shall be effective unless in writing. This Agreement may not be assigned by Customer without Unibeam's prior written consent.

For questions regarding this Agreement, please contact: [legal@unibeam.io](mailto:legal@unibeam.io)