WW SOFTWARE DEFENDER

Terms of Use — Fraud & Risk Intelligence API

Version 3.2 | Effective Date: August 26, 2026 | Replaces v3.1 (August 15, 2026)

READ CAREFULLY BEFORE USING THE SYSTEM.

By accessing, integrating, or using WW Software Defender via the official cloud instance or API, you fully accept these Terms of Use. If you do not agree with any clause, you must not use the Service.

1. Identification of the Owner

WW Software Defender is a system developed and maintained by Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender (hereinafter the "Company," "we," "us," or "our"). References in these Terms to "the Service" or "WW Software Defender" mean the platform, API, and related infrastructure described in Section 3.

Contact: kelsonfilipedev@gmail.com | Phone/WhatsApp: +244 947 151 042 | Production: https://ww-software-defender.vercel.app

These Terms use several role-based terms depending on context: "Account Holder" refers to an individual who registers for an Account (Free or paid) via the website; "Integrator" refers to an external system or entity integrating with the Service via the API; "Tenant" refers to a business entity with configured multi-user access; and "Customer" refers to any of the above when holding a paid Subscription. The same natural or legal person may hold more than one of these roles simultaneously.

2. Legal Capacity

By using WW Software Defender, the user expressly declares full legal capacity to enter into these Terms of Use on their own behalf or on behalf of the entity they represent, and that they possess the necessary internal authorizations to bind that entity.

3. Description of the System

WW Software Defender is a real-time fraud and risk-scoring engine that analyzes behavioral events, calculates risk scores, defines entity states, and triggers automated response actions

(Allow, Throttle, Challenge, Block), producing a complete and traceable audit trail.

The system operates the full cycle: Event -> Risk -> State -> Decision -> Action -> Audit

The system is available exclusively as a cloud/SaaS service — the official instance hosted across the Company's cloud infrastructure providers (see Section 9), accessible via API. The source code is proprietary and not publicly available.

WW Software Defender is a decision layer for fraud and abuse mitigation. It does not replace the integrator's own operational safeguards — internal processes, monitoring, or dedicated infrastructure security tooling — and is not a substitute for a complete and self-sufficient security solution.

3A. Payment Processor and Merchant of Record

Our order process is conducted by our online reseller Paddle.com. Paddle.com is the Merchant of Record for all our orders. Paddle provides all customer service inquiries and handles returns.

All paid Subscriptions are processed through Paddle.com Market Limited ("Paddle"), which acts as the Merchant of Record for all transactions. This means Paddle is the authorized reseller of the Service, is responsible for calculating, collecting, and remitting applicable sales tax, VAT, and similar consumption taxes, and handles order processing, invoicing, payment disputes, and chargebacks on the Company's behalf.

Your payment is subject to Paddle's Buyer Terms and Privacy Notice, available at paddle.com/legal, in addition to these Terms of Use. In case of conflict between these Terms and Paddle's terms regarding the processing of a payment transaction, Paddle's terms shall govern solely with respect to that transaction.

Refunds and cancellations are governed by our Refund Policy, available at https://ww-software-defender.vercel.app/legal/refund.

3B. Subscription Plans, Billing and Overage

WW Software Defender is offered under the following Subscription Plans, each with a monthly event allowance:

Plan	Monthly Fee	Included Events/Month	Overage Rate (per 1,000 events)	One-Time Setup Fee
Free	€0	5,000	Not applicable — no overage billing	Not applicable

Starter	€49	50,000	€1.50	None
Growth	€149	250,000	€1.00	€99 (see Section 3B(f))
Business	€399	1,000,000	€0.60	€299 (see Section 3B(f))

(a) Billing Cycle. Paid Subscriptions are billed monthly in advance, on a recurring basis, through Paddle, starting on the date of initial purchase.

(b) Overage Charges. If a Customer's usage exceeds the monthly event allowance of their Subscription Plan during a billing cycle, the excess events will be billed at the applicable Overage Rate as a one-time charge processed at the close of that billing cycle, in addition to the recurring Subscription Fee. Overage charges are calculated based on the Service's internal event counters and are non-negotiable absent a demonstrable system error.

(c) Failed Payments. If an overage charge or recurring Subscription Fee fails to process, Paddle will automatically retry the charge according to its standard retry schedule. The Company reserves the right to suspend or downgrade access to the Service if payment continues to fail after Paddle's retry attempts are exhausted, subject to Section 11 (Suspension and Revocation of Access).

(d) Free Plan. The Free Plan does not require payment method registration and carries no billing obligations. Usage exceeding the Free Plan's monthly event allowance may result in service throttling or a requirement to upgrade to a paid plan, at the Company's discretion, rather than overage billing.

(e) Price Changes. The Company may modify Subscription Plan pricing prospectively, with reasonable prior notice to active Customers. Price changes will not apply retroactively to a billing cycle already in progress.

(f) Setup Fees. Growth Plan Subscriptions include a one-time Setup Fee of €99, and Business Plan Subscriptions include a one-time Setup Fee of €299, each billed once via Paddle at the time of initial subscription to the respective plan, in addition to the first recurring Subscription Fee. The Setup Fee covers dedicated onboarding support to help the Customer configure and launch their integration.

The Setup Fee is not billed again on renewal, on a plan change within the same tier, or on reactivation of a Subscription that was continuously active without a lapse. If a Customer upgrades from Starter to Growth, or from Growth to Business, the Setup Fee applicable to the new, higher tier becomes payable at the time of the upgrade.

The Setup Fee is non-refundable once billed, except as set out in our Refund Policy.

3C. Cancellation

(a) Cancellation by Customer. Customers may cancel their paid Subscription at any time through their account settings or by contacting the Company. Cancellation will take effect at the end of the current, already-paid billing cycle. The Customer retains full access to the Service, at their current Subscription Plan tier, until the end of that billing cycle.

(b) No Immediate Termination of Access. Cancellation does not result in immediate loss of access. No partial-period or pro-rata refund is provided for the unused portion of a billing cycle following cancellation, except as required by applicable law or as described in our Refund Policy.

(c) Effect of Cancellation. Upon expiration of the final paid billing cycle, access to the Service, including the API, will be disabled, and the Customer's data may be retained or deleted in accordance with our Privacy Policy and Data Processing Agreement.

(d) Distinction from Suspension. This Section governs voluntary cancellation by the Customer. Suspension or revocation of access due to violation of these Terms is governed separately by Section 11 and does not entitle the Customer to any refund, whether partial or full.

4. Access Model and Users

Account Holders may register for an Account via the website's sign-up form, providing a name, company name, email address, and password. Registering an Account does not by itself grant end-user registration or login capabilities to the Integrator's own end-users — the Service does not provide a registration or login interface for the Integrator's end-users. Programmatic access to the Service is exclusively intended for external systems integrating via REST API using JWT or API Keys, and for Tenants previously configured in the system.

Authentication for API access is performed via two mechanisms: (a) JWT — obtained via POST /api/auth/token with valid clientId and apiKey; (b) Direct API Key — sent in the x-api-key header for enterprise integration without JWT.

Each tenant operates in an isolated PostgreSQL schema, ensuring data separation between clients. The integrator is entirely responsible for the configuration, interpretation, and use of decisions generated by the system.

5. Credential Security

The integrator is responsible for the confidentiality of their API Keys, JWT tokens, and any other access credentials. The integrator commits to: (a) not sharing credentials with unauthorized third parties; (b) storing API Keys securely, never in public source code; (c) immediately notifying the Company of any suspected credential compromise; (d) revoking and replacing credentials whenever a collaborator with access leaves the organization.

The Company is not responsible for unauthorized access resulting from credential compromise by the integrator.

6. No Warranty

The system is provided "as-is" and "as-available", without express or implied warranties of: continuous or uninterrupted availability; fitness for a specific purpose; absence of errors, failures, or vulnerabilities; complete detection of fraudulent or abusive behavior; universal compatibility with third-party systems; or absolute accuracy or reliability of automatic decisions.

The user expressly accepts that use of the system is at their own risk.

7. Data Collected and Stored

The system stores: (a) behavioral events — type, entityId, timestamp, and JSON payload; (b) risk scores (0–100) per entity; (c) entity states — NORMAL, SUSPICIOUS, ALERT, CRITICAL, BLOCKED; (d) automatic decisions — ALLOW, THROTTLE, CHALLENGE, BLOCK; (e) audit trail of all decisions.

The Service does not itself perform active geolocation derived from IP addresses or device fingerprinting. However, behavioral events, entity identifiers, and payloads submitted by the Customer to the Service may contain personal data (for example, IP addresses, user identifiers, or session identifiers), depending on how the Customer configures and uses the Service.

The Customer is solely responsible for the content of submitted payloads, including any personal data they contain, and represents that it possesses an adequate legal basis for the processing of such data under applicable data protection legislation, including the GDPR where applicable. Where the Service processes personal data on the Customer's behalf, such processing is governed by the Data Processing Agreement (DPA) available at https://ww-software-defender.vercel.app/legal/dpa, which forms part of these Terms for Customers subject to the GDPR or similar data protection laws.

8. Automatic Decisions and Actions

The system executes decisions automatically based on the risk score:

— Score 0–20 -> State NORMAL -> Action ALLOW

— Score 21–40 -> State SUSPICIOUS -> Action THROTTLE

— Score 41–60 -> State ALERT -> Action CHALLENGE

— Score 61–80 -> State CRITICAL -> Action BLOCK

— Score 81–100 -> State BLOCKED -> Action BLOCK

The system may automatically block: individual entities (by entityId); excess requests per entity (rate limiting via Redis, default: 30/minute); abusive IPs at network level (global ThrottlerGuard, default: 30 req/min).

The user accepts that automatic decisions may produce false positives or false negatives, and that the Company is not liable for undue blocks or failures to detect fraudulent or abusive activity.

9. Technical Limits and API Changes

The Company may apply technical limits on usage, throughput, or requests per minute to ensure operational stability, without prior notice. The Company may modify endpoints, payload structures, authentication mechanisms, or API versions for technical, operational, or security reasons.

The system's operation may depend on third-party services — including Render, Supabase, Upstash, and Vercel — over which the Company has no direct control.

10. Prohibited Use

The user is expressly prohibited from:

— using the system for illegal, fraudulent, or harmful purposes;

— attempting to circumvent authentication, rate limiting, or tenant isolation mechanisms;

— performing reverse engineering of the official cloud instance;

— executing stress tests or denial-of-service attacks without prior written authorization;

— using the system for illegal surveillance or unauthorized monitoring of individuals;

— attempting to extract credentials or data from other tenants;

— using the system as an offensive component in attacks against third parties;

— submitting payloads containing malicious code or exploits.

Violation of these prohibitions may result in immediate access suspension, without prejudice to applicable civil or criminal liability.

11. Suspension and Revocation of Access

The Company reserves the right, with prior notice where possible or immediately in cases of serious abuse, to: revoke API Keys of tenants violating these Terms; suspend access of tenants involved in abusive use; block IP addresses representing operational risk; discontinue the cloud service when operationally viable.

Suspension does not confer the right to any refund or compensation.

12. Availability and Service Level (SLA)

WW Software Defender is provided "as-is" and "as-available", without contractual guarantees of availability or minimum uptime. The cloud instance depends on third-party infrastructure and may experience interruptions due to maintenance, technical limitations, or failures outside the Company's control.

The user is responsible for implementing adequate fallback mechanisms in their integration systems.

13. Limitation of Liability

To the maximum extent permitted by applicable law, the Company shall not be liable for: direct, indirect, incidental, or consequential damages; undue automatic blocks; detection failures; data loss due to third-party infrastructure failures; cloud service unavailability; unpatched vulnerabilities; damages from incorrect API use or inadequate configuration; operational losses from automatic decisions; technical API changes; or credential compromise due to integrator negligence.

Cap on Direct Damages. To the maximum extent permitted by applicable law, the Company's total aggregate liability arising out of or related to these Terms, the Service, or any Subscription, whether in contract, tort, or otherwise, shall not exceed the total Subscription Fees actually paid by the Customer (via Paddle) in the twelve (12) months immediately preceding the event giving rise to the claim.

Free Plan. For Customers using the Free Plan, which is provided free of charge and without any payment obligation, the Company's total liability arising out of or related to the Free Plan shall be zero (€0), to the maximum extent permitted by applicable law.

This limitation applies regardless of the form of action and even if the Company has been advised of the possibility of such damages. Nothing in these Terms excludes or limits liability that cannot be excluded or limited under applicable law, including liability for death, personal injury, or fraud.

Relationship to the DPA liability cap. Where personal data is processed under the Data Processing Agreement (DPA), claims arising specifically from the Company's breach of its obligations as Processor under the DPA are governed exclusively by the liability cap set out in Section 12 of the DPA, including the EUR 500 cap applicable to Integrators on the Free Plan, rather than by the €0 Free Plan cap in this Section. All other claims under these Terms remain subject to this Section 13. See Section 12 of the DPA for details.

14. Data Protection and Access Controls

The system implements: dual authentication (JWT + API Keys with SHA-256 hashing); per-tenant data isolation via dedicated PostgreSQL schema; rate limiting per entity and per IP via Redis; audit trail with full traceability and integrity.

The user acknowledges that no system is absolutely infallible and that WW Software Defender does not guarantee detection of all fraudulent or abusive activity.

15. Intellectual Property

WW Software Defender and all its source code, architecture, documentation, and associated materials are proprietary and the exclusive property of the Company. All rights reserved.

The name "WW Software Defender" and associated branding are trademarks of the Company. No right to use the name, branding, or any part of the system is granted beyond the access expressly provided under these Terms.

16. Modifications to These Terms

The Company reserves the right to modify these Terms of Use, with prior notice published on the platform whenever operationally feasible. Continued use of the service after publication of new terms constitutes acceptance of the changes.

17. Severability

If any provision of these Terms is found to be invalid, illegal, or unenforceable by any competent court or authority, the remaining provisions shall remain fully valid and effective.

18. Governing Law and Jurisdiction

These Terms of Use are governed by the law of the Republic of Angola, without prejudice to applicable international standards, including the GDPR of the European Union where the integrator or processed data are subject to that regulation.

The courts of the District of Luanda, Republic of Angola, shall have exclusive jurisdiction, with express waiver of any other, to resolve any disputes arising from the interpretation or execution of these Terms.

19. Related Policies

These Terms of Use should be read together with the following policies, which form part of the agreement between the Customer and the Company:

— Privacy Policy — https://ww-software-defender.vercel.app/legal/privacy

— Refund Policy — https://ww-software-defender.vercel.app/legal/refund

— Data Processing Agreement (DPA) — https://ww-software-defender.vercel.app/legal/dpa

20. Contact

For questions regarding these Terms of Use, data protection, or support: Kelson Tchisseke Filipe Muiani, doing business as WW Software Defender | Email: kelsonfilipedev@gmail.com | Phone/WhatsApp: +244 947 151 042 (primary), +244 953 226 563 (secondary) | GitHub: github.com/kelsonFilipeDev