

**CODE109 LTD.**  
**BUG BOUNTY PROGRAM**  
TERMS AND CONDITIONS

LAST UPDATE DATE: June 1st 2026

PLEASE READ THESE TERMS AND CONDITIONS ("**AGREEMENT**") CAREFULLY BEFORE PARTICIPATING IN THE CODE109 BUG BOUNTY PROGRAM ("**PROGRAM**"). BY CLICKING "I AGREE" OR BY OTHERWISE PARTICIPATING IN THE PROGRAM, YOU ("**RESEARCHER**") AGREE TO BE LEGALLY BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT PARTICIPATE.

**1. DEFINITIONS**

As used in this Agreement, the following terms have the meanings set forth below:

- "**Agreement**" means these Terms and Conditions, as may be amended by Code109 from time to time upon notice to Researcher.
- "**Code109**" or "**Company**" means Code109 Ltd., a company incorporated under the laws of the State of Israel.
- "**Challenge Server**" means the designated, isolated testing environment accessible at <https://code109-beta.vercel.app/>, which constitutes the exclusive scope of authorized testing under this Program.
- "**Findings**" means any vulnerability, security flaw, bug, exploit, method, approach, technique, tool, or related information discovered or developed by Researcher in connection with the Program.
- "**Permitted Activities**" has the meaning set forth in Section 4.1.
- "**Program**" means Code109's bug bounty initiative as described in this Agreement.
- "**Researcher**" means the individual who has accepted this Agreement and is participating in the Program.
- "**Sensitive Data**" means any personal information, health information, financial information, credentials, source code, trade secrets, confidential business information, or other data that is subject to legal or contractual protection.
- "**Submission**" means any report, communication, or disclosure made by Researcher to Code109 in connection with the Program.

**2. ELIGIBILITY**

Participation in the Program is conditioned on Researcher meeting all of the following requirements at all times during participation:

- Researcher must be at least eighteen (18) years of age.
- Researcher must not be a resident of, or located in, any country or territory that is subject to comprehensive sanctions administered by the United States (including OFAC), the European Union, the State of Israel, or the United Nations, including but not limited to Iran, North Korea, Cuba, Syria, and Russia.
- Researcher must not be an employee, director, officer, contractor, subcontractor, agent, consultant, or immediate family member of any such person, of Code109 or any of its affiliated entities.
- Researcher must have the full legal capacity and authority to enter into this Agreement and to perform the obligations set forth herein.

- Researcher must not be prohibited by any applicable law or regulation from participating in the Program or receiving payment hereunder.

*Code109 reserves the right to verify eligibility at any time and to disqualify any Researcher who does not meet the foregoing requirements.*

### **3. ACCEPTANCE AND TERM**

This Agreement becomes effective upon Researcher's acceptance (by clicking "I AGREE" or equivalent digital acknowledgment) and continues until terminated in accordance with Section 12. Researcher's continued participation in the Program constitutes ongoing acceptance of all terms herein.

### **4. AUTHORIZED SCOPE AND PERMITTED ACTIVITIES**

#### **4.1. Permitted Activities**

Researcher is authorized solely to conduct the following activities, exclusively against the Challenge Server and for the purpose of identifying and responsibly disclosing genuine security vulnerabilities to Code109:

- Brute force, dictionary, and rainbow table attacks directed solely at the Challenge Server's authentication mechanisms.
- Credential stuffing against authentication endpoints on the Challenge Server.
- Reverse engineering of client-side JavaScript or compiled binaries served by or associated with the Challenge Server.
- Network interception and man-in-the-middle (MITM) analysis on Researcher's own isolated test network infrastructure, and solely in connection with traffic to or from the Challenge Server.
- Timing attacks and side-channel analysis directed at the Challenge Server.
- Social engineering, but only if and to the extent specifically coordinated and pre-approved in writing by Code109 via [Tsafrir@code109.com](mailto:Tsafrir@code109.com) prior to any such activity. Any approval is narrow, revocable, and specific to the agreed scenario.

All Permitted Activities must be conducted in good faith, for the sole purpose of identifying genuine security vulnerabilities, and in strict compliance with this Agreement and all applicable laws.

#### **4.2. Exclusivity of Authorized Scope**

The Challenge Server is the sole and exclusive authorized target under this Program. Researcher has no authorization, express or implied, to test, probe, scan, access, or interact with any other Code109 system, server, service, application, network, infrastructure, database, or device, or any third-party system, whether or not owned or operated by Code109 or its service providers.

### **5. PROHIBITED ACTIVITIES**

Without limiting any other provision of this Agreement, and in addition to any activities not expressly listed as Permitted Activities under Section 4, the following activities are strictly prohibited. Researcher shall not, under any circumstances:

#### **5.1. Technical Prohibitions**

- Conduct or attempt any Denial of Service (DoS), Distributed Denial of Service (DDoS), or any other attack or technique that intentionally or foreseeably degrades, disrupts, impairs, or interferes with the availability, performance, or integrity of the Challenge Server, any Code109 system, or any third-party infrastructure.
- Deface, modify, alter, delete, or destroy any data, content, configuration, or functionality on the Challenge Server beyond the minimum required for a proof-of-concept demonstration of a vulnerability.

- Access, view, copy, exfiltrate, retain, transmit, sell, publish, or otherwise process or exploit any data belonging to other participants or any other person, including any Sensitive Data, beyond what is strictly necessary to document the existence of a vulnerability.
- Deploy or introduce malware, ransomware, cryptominers, persistence mechanisms, backdoors, web shells, destructive payloads, or any unauthorized code or software on the Challenge Server or any other system.
- Perform physical attacks, hardware attacks, or any form of unauthorized physical access (noting that the Challenge Server is cloud-hosted and no physical access is possible or authorized).
- Attack, probe, scan, or interact with any system, server, or infrastructure other than the Challenge Server, including but not limited to Code109's production systems, client systems, partner systems, or any third-party systems.
- Use credential stuffing, phishing, pretexting, or social engineering against any person or system except as specifically pre-authorized in writing by Code109 under Section 4.1(f).

## **5.2. Conduct Prohibitions**

- Engage in unlawful, unauthorized, fraudulent, deceptive, coercive, extortionate, threatening, abusive, or otherwise improper conduct in connection with the Program or any Submission.
- Attempt to leverage, use, or threaten the use of any Findings, Submission, or participation in the Program to extract payment, concessions, or any benefit from Code109 or any third party beyond the bounty expressly offered under this Program.
- Contact, disclose information to, or communicate with any of Code109's customers, business partners, regulators, press, media, or other third parties regarding any Findings, Submission, or participation in the Program.
- Threaten, imply, or take any action constituting publicity, regulator reporting, reputational harm, legal action, or commercial pressure for the purpose of obtaining payment or any other benefit.
- Represent to any third party that Code109 authorizes, endorses, directs, sponsors, or is affiliated with Researcher's activities beyond what is expressly stated in this Agreement.
- Engage in any activity that is illegal under the laws of the State of Israel, the laws of Researcher's jurisdiction, or any other applicable law, including but not limited to applicable computer fraud, data protection, privacy, export control, and sanctions laws.
- Retain, use, or disclose Sensitive Data beyond what is strictly necessary to document the relevant Findings and solely to the extent permitted by law and this Agreement.
- Publish, disclose, discuss, or share any exploit code, Findings, or information relating to any vulnerability prior to the expiration of the Embargo Period defined in Section 9, or without Code109's prior written approval.

## **6. SENSITIVE DATA AND SECURITY INCIDENT ESCALATION**

If Researcher becomes aware, or reasonably suspects, that any activity in connection with the Program has resulted in or may result in any of the following, Researcher shall immediately (and in any event within two (2) hours of becoming aware):

- Access to, or inadvertent exposure of, Sensitive Data;
- System compromise, establishment of persistence, or unauthorized control over any system;
- Service degradation or disruption affecting any system;
- Evidence of access to any system by another unauthorized actor; or

- Any circumstances that could reasonably constitute an actual or suspected security incident (as opposed to merely the discovery of a vulnerability).

Upon becoming aware of any such circumstances, Researcher shall:

- Immediately cease all further activity except to the minimum extent required to preserve evidence, and only where lawful to do so;
- Take no further action that would expand access, exposure, or impact;
- Promptly report the matter to Code109 via [hack@code109.com](mailto:hack@code109.com), providing all relevant details; and
- Cooperate fully with Code109's incident response and investigation.

Researcher shall not retain, use, disclose, transmit, analyze, or otherwise process any Sensitive Data beyond what is strictly necessary to document the relevant security issue and only where permitted by law and this Agreement.

Code109 may immediately suspend review, communications, payment consideration, or all of Researcher's participation under the Program, pending legal or incident-response review, without incurring any liability to Researcher.

## 7. SUBMISSIONS AND REPORTING REQUIREMENTS

### 7.1. Submission Requirements

All Findings must be submitted exclusively by email to [Tsafrir@code109.com](mailto:Tsafrir@code109.com). As a condition of eligibility for any bounty payment and as a mandatory contractual obligation, each Submission must include, to the extent legally and contractually permissible, each of the following:

- Identification of the applicable Challenge Server and the specific component, endpoint, or functionality affected;
- A detailed description of the vulnerability, including its type, nature, and root cause;
- Identification of the affected product, service, or system component;
- The date of discovery;
- The date and method of initial disclosure to Code109;
- Confirmation that the vulnerability falls within the authorized scope of the Program;
- Evidence sufficient for Code109 to assess the quality, severity, and usability of the Submission, including without limitation steps to reproduce, screenshots, screen recordings, or proof-of-concept scripts or code;
- A complete and accurate disclosure of all methods, techniques, approaches, tools, software components, libraries, exploits, and other resources used in connection with discovery of the vulnerability;
- Any known restrictions on publication, attribution, timing, or third-party rights;
- If known, the remediation status; and
- Researcher's full legal name, contact information, and any payment details required pursuant to Section 8.

### 7.2. Cooperation Obligation

Researcher agrees to respond promptly and fully to any follow-up questions from Code109 regarding any Submission, and to provide any additional information, evidence, or cooperation reasonably requested by Code109 in connection with the verification, assessment, or remediation of any Findings. This obligation continues after payment of any bounty.\

### **7.3. Response Time**

Code109 will Endeavor to acknowledge receipt of a Submission within four reenable time of receipt on a working week basis. This is a target only and does not constitute a binding commitment.

### **7.4. First Reporter / Duplicate Submissions**

In the event that two or more Researchers report the same valid vulnerability, the following rules apply:

- The Researcher whose Submission is received first by Code109 is deemed the "First Reporter" and is eligible for the full bounty.
- If two Submissions reporting the same vulnerability are received within a twenty-four (24) hour window of each other, Code109 may, in its sole discretion, elect to split the applicable bounty equally between the two Researchers. This is a discretionary accommodation and not a right of either Researcher.
- Code109's determination as to the identity of the First Reporter and the existence of duplicate Submissions is final and binding.

## **8. BOUNTY PAYMENT**

### **8.1. Bounty Amount**

The bounty amount is published by Code109 on social. That amount may change, from time to time, at Code109's sole discretion.

### **8.2. Payment Conditions**

Payment of any bounty is subject to all of the following conditions being satisfied:

- Researcher is the First Reporter of the vulnerability.
- Researcher has submitted a complete and compliant Submission in accordance with Section 7;
- Code109 has verified the validity and scope-compliance of the Findings;
- Researcher has answered all follow-up questions and provided all additional information requested by Code109;
- Researcher has complied with all terms of this Agreement, including the Embargo Period;
- Researcher has provided valid payment details acceptable to Code109;
- Researcher has issued to Code109 a valid tax invoice, as per the requirements of Code109; and
- No grounds for disqualification exist under this Agreement.

### **8.3. Payment Timeline and Method**

Subject to satisfaction of the conditions in Section 8.2, Code109 will Endeavor to pay any verified bounty within sixty (60) calendar days after verification & approval. Payment will be made by one of the following methods, at Code109's election: PayPal, Visa, USDC (cryptocurrency), or international bank wire transfer. Code109 reserves the right to request additional information (including identification information and tax documentation) prior to processing payment.

### **8.4. Taxes**

Researcher is solely responsible for all taxes, levies, duties, and withholdings (including income tax, self-employment tax, VAT, and any other applicable taxes) arising from or relating to any payment received under this Program, except to the extent non-waivable applicable law requires Code109 to withhold or remit any amounts. Code109 makes no representation regarding the tax treatment of any payment in any jurisdiction. Bounty amount includes all taxes, including VAT, sales taxes, and any other tax.

### **8.5. No Other Compensation**

Except for any bounty expressly verified and approved by Code109 in accordance with this Agreement, Researcher is not entitled to any compensation, remuneration, reimbursement, or other payment from Code109 in connection with the Program, including for time spent, expenses incurred, or any other basis.

## **9. DISCLOSURE EMBARGO**

### **9.1. Embargo Period**

Researcher agrees to maintain strict confidentiality regarding all Findings and shall not, directly or indirectly, disclose, publish, distribute, discuss, or communicate any information relating to any Findings to any person or entity (including on any social media, blog, forum, conference, or other public platform) until the later of: (a) ninety (90) calendar days after the official end of the Program campaign; or (b) Code109's public deployment of a fix for the relevant vulnerability (the "**Embargo Period**"). To enforce this right Code109 may determine that all or part of the bounty payment shall be made following the Embargo Period.

### **9.2. Early Disclosure Consequences**

Any disclosure of Findings prior to the expiration of the Embargo Period, or without Code109's prior express written approval, shall: (a) result in immediate forfeiture of any bounty associated with the relevant Submission; (b) constitute a material breach of this Agreement; and (c) may result in Code109 pursuing all available legal remedies, including injunctive relief and claims for damages.

### **9.3. Approved Publications**

Code109 may, in its sole and absolute discretion, approve a Researcher's request to publish information regarding Findings prior to the end of the Embargo Period. Any such approval must be in writing and signed by an authorized representative of Code109. Any approved publication must:

- Be submitted to Code109 for review and written approval at least fourteen (14) calendar days prior to publication;
- Prominently reference Code109 by name and include a link to Code109's website;
- Reference the Program and the nature of the Findings (subject to Code109's redaction requirements);
- Not disparage, defame, or make any negative, misleading, or derogatory statements regarding Code109, its products, services, personnel, clients, or affiliates;
- Not include any content that could reasonably be expected to damage Code109's reputation or business relationships; and
- Comply with all applicable laws and platform terms of service.

Code109 reserves the right to require modifications to any proposed publication as a condition of approval. Researcher shall incorporate all requested changes prior to publication.

## **10. INTELLECTUAL PROPERTY; LICENSE GRANTS**

### **10.1. Assignment of Findings**

To the maximum extent permitted by applicable law, Researcher hereby irrevocably assigns to Code109 all right, title, and interest (including all intellectual property rights) in and to all Findings, including all discoveries, inventions, methods, techniques, analyses, and improvements arising from or related to Researcher's activities under this Program. Researcher has no, and hereby irrevocably and unconditionally waives any, right to receive any additional payment, royalty or any other payment or compensation from Code109 or anyone related to it, in connection with the

Findings and all of the foregoing. To the extent any such assignment is not effective as a matter of law, Researcher grants to Code109 the license set forth in Section 10.2.

**10.2. License to Findings**

To the extent that any right, title, or interest in any Findings cannot be assigned, Researcher hereby grants to Code109 an exclusive, irrevocable, perpetual, worldwide, fully paid-up, royalty-free license, with the right to sublicense through multiple tiers, to use, reproduce, modify, adapt, translate, distribute, display, perform, create derivative works from, and otherwise exploit any Findings in any manner and for any purpose, including without limitation for improving, developing, commercializing, and providing Code109's products and services (the "**Findings License**"). The Findings License is granted without any right of attribution or moral rights in favor of Researcher, and Researcher hereby irrevocably waives any moral rights or rights of attribution in connection with the Findings to the maximum extent permitted by applicable law.

**10.3. License to Name, Image, and Likeness**

Researcher irrevocably grants to Code109 a perpetual, worldwide, royalty-free, sublicensable right and license to use Researcher's name, photograph, image, likeness, username, social media handle, and any other biographical or identifying information provided by Researcher, for the purposes of identifying Researcher as a participant in the Program, identifying Researcher as a bounty recipient or winner (if applicable), and promoting and publicizing the Program and Code109's products and services, in any media, format, or channel, whether now known or hereafter developed. This license does not obligate Code109 to make any use of Researcher's name, image, or likeness.

**10.4. No Reverse License**

Nothing in this Agreement grants Researcher any license or right in or to Code109's intellectual property, products, services, or systems, beyond the narrow authorization to conduct Permitted Activities set forth in Section 4 during the term of the Program.

**10.5. Feedback**

Any suggestions, feedback, ideas, or comments provided by Researcher to Code109 in connection with the Program (including without limitation as part of any Submission or communication) are provided on a non-confidential basis (except as otherwise provided in Section 11), and Code109 shall have the same exclusive, irrevocable, perpetual, worldwide, fully paid-up, royalty-free ownership rights and license to use such feedback as set forth in Sections 10.1 and 10.2 above.

**11. CONFIDENTIALITY**

**11.1. Mutual Confidentiality**

All communications, correspondence, and information exchanged between Code109 and Researcher in connection with the Program (including without limitation the substance of any Submission, the existence or status of any review or payment, and any technical information shared by Code109) are strictly confidential and may not be disclosed to any third party without the prior written consent of the disclosing party.

**11.2. Researcher's Obligations**

Researcher shall:

- Hold all confidential information of Code109 in strict confidence using at least the same degree of care Researcher uses to protect Researcher's own confidential information, but in no event less than reasonable care;
- Use confidential information of Code109 solely for the purpose of performing activities authorized under this Agreement;
- Not disclose any confidential information of Code109 to any third party; and
- Promptly notify Code109 upon becoming aware of any actual or suspected unauthorized disclosure of Code109's confidential information.

### **11.3. Exceptions**

The confidentiality obligations in this Section 11 do not apply to information that: (a) is or becomes generally available to the public through no breach of this Agreement by Researcher; (b) was rightfully known to Researcher prior to disclosure by Code109 without restriction; (c) is rightfully obtained by Researcher from a third party without restriction; or (d) is required to be disclosed by applicable law or court order, provided that Researcher provides Code109 with prompt written notice (to the extent legally permissible) and reasonably cooperates with Code109's efforts to seek a protective order or other appropriate relief.

## **12. LIMITED SAFE HARBOR; NO LEGAL ADVICE OR WARRANTY**

### **12.1. Limited Safe Harbor**

Subject to Researcher's full compliance with this Agreement, Code109 agrees that it will not pursue civil legal action against Researcher solely for conduct that constitutes Permitted Activities under Section 4 of this Agreement and that does not violate any applicable law. For the avoidance of doubt, this commitment:

- Does not apply to any activity that violates this Agreement, falls outside the scope of Permitted Activities, or is otherwise prohibited under Section 5;
- Does not apply to any activity that constitutes a criminal offense or that violates any applicable law in any jurisdiction;
- Does not bind any third party, including any government authority, law enforcement agency, or other individual or entity;
- Does not constitute a waiver of any rights of Code109 with respect to criminal conduct or unauthorized activity; and
- Does not obligate Code109 to refrain from cooperating with law enforcement or regulatory authorities.

### **12.2. No Legal Advice**

RESEARCHER ACKNOWLEDGES AND AGREES THAT CODE109 DOES NOT PROVIDE, AND NOTHING IN THIS AGREEMENT OR THE PROGRAM CONSTITUTES, LEGAL ADVICE OR ANY REPRESENTATION OR WARRANTY OF ANY KIND REGARDING THE LEGALITY OF RESEARCHER'S ACTIVITIES IN ANY JURISDICTION WORLDWIDE. CODE109 EXPRESSLY MAKES NO REPRESENTATION THAT PARTICIPATION IN THE PROGRAM PROTECTS RESEARCHER FROM ANY CLAIM, LIABILITY, INVESTIGATION, OR PROSECUTION UNDER ANY APPLICABLE LAW IN ANY JURISDICTION, INCLUDING WITHOUT LIMITATION:

- The Computer Fraud and Abuse Act of 1986 (CFAA) or any similar state or foreign computer fraud or cybercrime law;
- The Digital Millennium Copyright Act (DMCA) or any equivalent copyright law;
- Any privacy or data protection law, including the GDPR, Israel's Privacy Protection Law (5741-1981), or the California Consumer Privacy Act (CCPA);
- Any trade secret law, including the Defend Trade Secrets Act (DTSA);
- Any export control or sanctions law; or
- Any other applicable federal, state, national, or local law or regulation.

RESEARCHER IS SOLELY RESPONSIBLE FOR ENSURING THAT ALL OF RESEARCHER'S ACTIVITIES IN CONNECTION WITH THE PROGRAM COMPLY WITH ALL APPLICABLE LAWS AND REGULATIONS IN ALL RELEVANT JURISDICTIONS. RESEARCHER IS STRONGLY ENCOURAGED TO CONSULT WITH QUALIFIED LEGAL COUNSEL BEFORE PARTICIPATING IN THE PROGRAM.

### **13. RESEARCHER'S REPRESENTATIONS, WARRANTIES, AND COVENANTS**

Researcher represents, warrants, and covenants to Code109, on a continuing basis throughout the term of this Agreement, that:

- Each Submission arises from lawful and authorized activity conducted in compliance with this Agreement and all applicable laws and regulations;
- Researcher has not and will not rely on Code109 as a source of authorization to conduct testing, access any system, or engage in any other activity;
- Researcher has complied with and will continue to comply with all applicable laws and regulations in all relevant jurisdictions;
- Researcher has accurately identified the applicable scope, circumstances, and relevant facts in connection with each Submission;
- Researcher has the full legal right and authority to submit each Submission to Code109 and to grant all rights set forth in Section 10;
- No Submission, and no use thereof by Code109 as permitted herein, knowingly infringes, misappropriates, or violates any third-party intellectual property right, privacy right, or other right;
- Researcher has not engaged and will not engage in extortionate, coercive, threatening, or ransom-like conduct in connection with the Program;
- Researcher has not intentionally introduced malicious code, established persistence, or caused or contributed to service disruption in connection with the Program;
- Researcher has not retained or misused Sensitive Data beyond what was strictly necessary and lawful;
- Researcher will comply with all publication restrictions, embargo requirements, and coordinated disclosure obligations applicable to any Submission; and
- Researcher is solely responsible for all taxes arising from any payment received under the Program, except to the extent non-waivable law requires Code109 to withhold or remit amounts.

### **14. INDEPENDENT STATUS; NO EMPLOYMENT RELATIONSHIP**

Researcher is an independent individual acting in Researcher's personal capacity. Nothing in this Agreement creates, or shall be construed to create, any employment, agency, partnership, joint venture, franchise, service provider, or similar relationship between Researcher and Code109. Researcher has no authority to bind Code109 to any obligation and shall not represent to any third party that any such relationship exists. Researcher is solely responsible for all employment taxes, withholdings, insurance, and other obligations arising from Researcher's own activities.

### **15. PROGRAM TERMINATION AND SUSPENSION**

Code109 may terminate or suspend the Program, in whole or in part, at any time, with or without notice, including but not limited to in the following circumstances:

- Discovery of a critical unpatched vulnerability that Code109 determines poses a risk to production systems or third parties;
- A legal, regulatory, or compliance requirement;
- Force majeure (including acts of God, war, civil unrest, governmental action, pandemic, or other events beyond Code109's reasonable control); or
- Any other reason in Code109's sole discretion.

In the event of termination of the Program, Code109 will use reasonable efforts to process and pay the 1st approval hacker Submissions that were received and verified as valid prior to the effective date of

termination, subject to all other conditions of this Agreement. Termination of the Program does not affect the continuing obligations of Researcher under Sections 10, 11, 12.2, 13 and 16, which shall survive termination.

## **16. DATA PROTECTION**

Code109 will collect and process Researcher's personal data (including name, contact information, and payment details) solely for the purposes of administering the Program, verifying Submissions, processing payments, and exercising Code109's rights under this Agreement. Code109 will not share Researcher's personal data with third parties without Researcher's consent, except as required by applicable law or legal process. If Researcher requests anonymity in connection with any public acknowledgment, Code109 will use reasonable efforts to honor such request, subject to Code109's legal obligations.

By participating in the Program, Researcher consents to the collection and processing of Researcher's personal data as described in this Section and as set forth in Code109's Privacy Policy (if applicable).

## **17. DISCLAIMERS**

- 17.1. THE PROGRAM IS PROVIDED "AS IS" AND "AS AVAILABLE," WITHOUT WARRANTY OF ANY KIND.
- 17.2. CODE109 MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, THAT ANY SUBMISSION WILL BE REVIEWED, ACCEPTED, USED, COMPENSATED, PUBLISHED, CREDITED, OR RESULT IN ANY COMMERCIAL BENEFIT TO RESEARCHER.
- 17.3. CODE109 DOES NOT WARRANT THAT PARTICIPATION IN THE PROGRAM PROTECTS RESEARCHER FROM ANY CLAIM BY ANY THIRD PARTY, GOVERNMENT AUTHORITY, OR LAW ENFORCEMENT AGENCY IN ANY JURISDICTION.
- 17.4. CODE109 EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

## **18. LIMITATION OF LIABILITY**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL CODE109 BE LIABLE TO RESEARCHER FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, OR FOR ANY LOSS OF PROFITS, REVENUE, DATA, OR GOODWILL, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE PROGRAM, EVEN IF CODE109 HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CODE109'S AGGREGATE LIABILITY TO RESEARCHER FOR ALL CLAIMS ARISING UNDER THIS AGREEMENT SHALL NOT EXCEED THE AMOUNT OF THE BOUNTY, IF ANY, ACTUALLY PAID BY CODE109 TO RESEARCHER UNDER THIS AGREEMENT.

## **19. INDEMNIFICATION**

Researcher shall defend, indemnify, and hold harmless Code109 and its officers, directors, employees, shareholders, affiliates, successors, and assigns from and against any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with: (a) Researcher's participation in the Program; (b) any breach of this Agreement by Researcher; (c) Researcher's violation of any applicable law or regulation; (d) Researcher's infringement or misappropriation of any third-party right; or (e) Researcher's negligence or willful misconduct.

## **20. GOVERNING LAW AND JURISDICTION**

This Agreement shall be governed by and construed exclusively in accordance with the laws of the State of Israel, without regard to its conflict of laws principles. Any dispute, claim, or controversy

arising out of or in connection with this Agreement or the Program shall be submitted to the exclusive jurisdiction of the competent courts located in Tel Aviv, Israel. Researcher irrevocably submits to the personal jurisdiction of such courts and waives any objection to venue in such courts.

## 21. GENERAL PROVISIONS

- 21.1. Entire Agreement. This Agreement constitutes the entire agreement between Researcher and Code109 with respect to the Program and supersedes all prior or contemporaneous agreements, representations, warranties, and understandings.
- 21.2. Amendment. Code109 reserves the right to amend this Agreement at any time by posting an updated version or providing notice to Researcher. Researcher's continued participation in the Program following notice of any amendment constitutes acceptance of the amended Agreement.
- 21.3. Severability. If any provision of this Agreement is found to be invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions shall continue in full force and effect.
- 21.4. Waiver. No failure or delay by Code109 in exercising any right under this Agreement shall constitute a waiver of such right.
- 21.5. Assignment. Researcher may not assign this Agreement or any rights or obligations hereunder without Code109's prior written consent. Code109 may assign this Agreement freely.
- 21.6. Notices. All notices required or permitted under this Agreement shall be in writing and delivered to Code109 by email to [Tsafrir@code109.com](mailto:Tsafrir@code109.com) (for program-related matters) or to the contact information provided at Code109's website.
- 21.7. Language. This Agreement is written in English. In the event of any conflict between an English version and any translation, the English version shall control.
- 21.8. Headings. Section headings are for convenience only and shall not affect the interpretation of this Agreement.

### ACKNOWLEDGMENT AND ACCEPTANCE

BY CLICKING "I AGREE" OR BY OTHERWISE PARTICIPATING IN THE PROGRAM, RESEARCHER ACKNOWLEDGES THAT RESEARCHER HAS READ THIS AGREEMENT IN ITS ENTIRETY, UNDERSTANDS ITS TERMS, HAS HAD THE OPPORTUNITY TO CONSULT WITH LEGAL COUNSEL, AND AGREES TO BE BOUND BY ALL OF ITS TERMS AND CONDITIONS.