Project Support Grant Agreement
from Open Sats Initiative, Inc. (EIN 85-2722249)

Date of Agreement:
Grantee:
ID#:
Purpose of Grant: **See Exhibit A containing Grantee's Proposal**
Total Amount of Grant:
Date of Award:
Project Period:
Payment Schedule:

This grant (the "Grant") is hereby awarded by Open Sats Initiative, Inc. (EIN: 85-2722249), a Texas not-for-profit corporation and 501(c)(3) public charity, (the "Initiative"), to the recipient, _____ , (the "Grantee"), subject to the following terms and conditions:

A. The Grant must be used solely for the purpose identified in the Grantee's proposal, and may not be expended for any other purposes without the Initiative's prior written approval. Any material change in scope or purpose to Grantee's approved project must receive advanced written permission from the Initiative. For avoidance of doubt, Grantee may not use the Grant to pay finder's fees, commissions, or percentage compensation to a fundraising professional, staff, consultant, or other organization. Furthermore, Grantee shall not use any portion of the Grant to participate or intervene in any political campaign on behalf of or in opposition to any candidate for public office or political party, to induce or encourage violations of law or public policy, to cause any private inurement or improper private benefit to occur, to take any other action inconsistent with Code Section 501(c)(3), to undertake any activity for any purpose other than a charitable, scientific, or educational purpose within the meaning of Code Section 170(c)(2)(B), or to attempt to influence legislation within the meaning of Code Section 501(c)(3). Unless specifically agreed to by the Initiative in writing, Grantee shall not disburse grant funds to any recipient acting as a fiscal sponsor or agent and shall not otherwise assign this grant agreement without the prior written consent of the Initiative.

B. Grantee shall provide the Initiative with periodic written reports including (a) a description of the progress that Grantee has made toward achieving the Grant Purposes; (b) an accounting of Grantee's expenditure of Grant funds; (c) copies of any publications resulting from the Grant; and (d) such additional information, reports, and documents as

the Initiative may reasonably request. Unless Exhibit A expressly specifies a reporting schedule for the Grant, the following standard reporting periods apply:

- First-time OpenSats grantee: 30-day progress report for the first three months of the Project Period. After that, 90-day reports every three months.

- Returning OpenSats grantee (second or subsequent grant): 90-day progress report every three months of the Project Period.

Where Exhibit A expressly specifies a reporting schedule for the Grant, that schedule supersedes the standard reporting periods set forth above, provided that no such schedule shall require reports less frequently than once every six (6) months. Each report due under such a schedule is subject to the remainder of this Section B.

Grantee acknowledges that any failure to submit a report by the end of the month in which it is due or, where Exhibit A specifies a reporting schedule, within fifteen (15) days after the date the report is due or such other period as Exhibit A specifies, shall trigger the immediate suspension of all further grant payouts until all outstanding reports have been submitted in full. Such failure may also result in the termination of the grant.

Grantee also acknowledges that the Initiative may request, and the Grantee must provide, documentation supporting the use of Grant proceeds including, but not limited to, receipts, invoices, bank statements, and credit card statements. Grantee further acknowledges that failure to provide requested information may result in termination of the Grant.

C. Grantee acknowledges that the Initiative strives to maintain an ecosystem of free and open-source (FOSS) contributors to Bitcoin and related FOSS projects, free and open-source software, and to support various charitable and education-related initiatives around Bitcoin and complementary FOSS tools and initiatives. As such, all code, software, applications, projects, initiatives, materials, and the like, developed or enhanced by Grantee, as part of Grantee's project for the Initiative, shall be shared with the Initiative and posted on Github or other similar publicly accessible sharing site approved by the Initiative's board of directors and such code shall free to access, or accessible and usable under a free and open-source license. Notwithstanding the foregoing, Grantee shall withhold from any public posting, publication, or other disclosure any vulnerability details, proof-of-concept or exploit code, or other information sufficient to enable exploitation of an unremediated security vulnerability, until public disclosure is permitted under Section I.

D. If Grantee is a scientific or research institution that is legally required to disclose supporters, the Initiative asks that this support be recognized as a grant and list the Initiative as "OpenSats Initiative". Grantee agrees to permit the Initiative to include and/or disseminate information about the grant and/or Grantee in its publications and communications, both print and electronic.

E. The Initiative reserves the right to discontinue, withhold, or modify the entirety or any part of the Grant award if in the Initiative's sole discretion, such action is necessary because: (i) Grantee becomes unable to carry out the purposes of the Grant, (ii) Grantee breaches this Agreement, including by using Grant funds for any purpose other than those set out in Grantee's Grant Proposal; (iii) to protect the reputation or tax-exempt status of the Initiative; (iv) a mistaken payout was made; or (v) to comply with any law or regulation applicable to the Grantee, to the Initiative, or to the Grant.

F. If the Grant is terminated prior to the scheduled completion date of the Project Period for any reason, upon Initiative's request, Grantee shall provide the Initiative a full accounting of the receipt and disbursement of funds and expenditures incurred under the grant as of the effective date of termination, and return any unused grant funds. The Initiative may request that Grantee return any unexpended grant funds remaining at the end of the Project Period, or at any time if the Grantee ceases to work on or fails to complete project obligations set out in the Grantee's Proposal. Should any Grant funds remain unspent under such circumstances, Grantee will contact the Initiative to discuss options including extending the Project Period, returning grant funds, and/or other options.

G. Grantee shall promptly notify the Initiative in writing if: (i) there is any change in circumstances that might affect Grantee's ability to carry out the Grant; (ii) Grantee undergoes a merger, division, or other corporate reorganization; (iii) Grantee becomes subject to a proceeding under the Bankruptcy Code or other law relating to insolvency or makes an assignment for the benefit of creditors; (iv) Grantee becomes subject to an investigation or proceeding brought by the Internal Revenue Service, Attorney General, any other regulatory agency, or any governmental unit whether located within the United States or without; or (v) Grantee receives notice of any litigation or other legal action relating to the grant or are served with a subpoena or other legal process seeking to compel production of or obtain access to any data related to the grant. Upon the occurrence of any of the events described in this Section, the Initiative reserves the right, at its option, to unilaterally amend the terms of the grant, including the right to terminate the grant. In the event that Grantee wishes to pause work on Grantee's Project for any reason, Grantee may contact the Initiative, which will pause the Grant until Grantee is ready to resume work.

H. Grantee shall take reasonable efforts, including, if applicable, engaging qualified regulatory counsel, to make sure that no aspect of Grantee's activities in relation to the Grant violate applicable laws or regulations, including, without limitation, laws pertaining to fraud, money laundering, terrorism financing, money services businesses, and export controls. The Grantee shall also take reasonable efforts to ensure that no aspect of Grantee's activities or use of Grant proceeds violates or evades U.S. and international sanctions laws and regulations. To the extent that Grantee is unsure whether such laws or regulations apply to Grantee's activities, Grantee should consult qualified independent counsel.

   Grantee shall not knowingly use or disclose nonpublic information obtained through the Grant or Grantee's relationship with the Initiative for the purpose of identifying, exposing,

harassing, or compromising another grantee or contributor, including by publicly associating a pseudonymous person with a legal identity or disclosing nonpublic personal information, wallet addresses, grant information, or similar information. This restriction does not prohibit disclosures required by law or good-faith reports of suspected misconduct or security threats to the Initiative, affected parties, legal counsel, or appropriate governmental authorities. A violation of this provision constitutes grounds for suspension or termination of the Grant and the exercise of any other remedies available to the Initiative under Sections E and F.

I. **Security Research and Responsible Disclosure.** This Section applies to the extent that Grantee's project involves security research, vulnerability testing, penetration testing, red-teaming exercises (including exercises using large language models or other artificial intelligence systems), or any other activity that could reasonably be expected to identify security vulnerabilities in any software, protocol, network, or system, including Bitcoin, Nostr, and related free and open-source software projects.

(1) Authorized Testing Only. Grantee shall conduct security and vulnerability testing only (a) against systems, networks, nodes, and software instances that Grantee owns or controls, including local test environments, private forks, testnets, signets, and regtest networks, or (b) against third-party systems with the prior authorization of the owner or operator of those systems or within the published scope of the affected project's security research, coordinated disclosure, or bug bounty policy. Grantee shall not (i) test against production systems, mainnet deployments, or live user-facing infrastructure without such authorization; (ii) access, alter, exfiltrate, destroy, or place at risk any data, funds, or other property of any third party; (iii) degrade or disrupt the availability of any third-party system or network; or (iv) engage in social engineering, phishing, or physical intrusion directed at any third party. Grantee shall conduct all activities under this Section consistent with accepted principles of good-faith security research and in compliance with applicable law, including the U.S. Computer Fraud and Abuse Act and analogous state, federal, and foreign laws. Regardless of whether Grantee is conducting testing, Grantee shall not access, move, transfer, sweep, or take custody or control of any funds, private keys, credentials, data, or other property of any third party. A good-faith belief that such action is necessary to protect the owner or to prevent loss does not constitute authorization. Grantee may take such action only with the express prior authorization of the owner of the funds, data, or other property, or where required by an order of a court or other governmental authority of competent jurisdiction.

(2) Reporting to Affected Parties. Upon identifying a security vulnerability, Grantee shall promptly and confidentially report it to the maintainers, developers, or vendor of the affected software, protocol, or system (the "**Affected Party**") through the Affected Party's designated security contact or published disclosure process or, if none exists, through other reasonably secure and confidential means. Reports shall include sufficient technical detail for the Affected Party to reproduce, assess, and remediate the

vulnerability. Where no maintainer, developer, or vendor can be identified after reasonable efforts, or where no reasonably secure channel is available, Grantee may report the vulnerability to a recognized vulnerability coordination body of Grantee's choosing. Grantee shall create and retain contemporaneous records sufficient to establish the date and content of each report and each material communication with the Affected Party under this Section, including copies of the communications themselves, and shall retain those records for at least three (3) years after the later of public disclosure of the vulnerability and the end of the Project Period. Grantee may, and is encouraged to, further evidence the existence and timing of such records through cryptographic timestamping or a similar mechanism.

(3) Coordinated Disclosure. Grantee shall not publicly disclose any vulnerability, or any information sufficient to enable its exploitation, except in accordance with this Section. Grantee shall follow the Affected Party's published coordinated disclosure policy, if any. In the absence of such a policy, Grantee shall not publicly disclose the vulnerability before the earlier of (a) the date on which a fix or mitigation has been released and a reasonable period for adoption has elapsed, or (b) ninety (90) days after Grantee's initial report to the Affected Party, and shall extend that period for a reasonable time where the Affected Party is making good-faith progress toward remediation or where the severity of the vulnerability and the complexity of remediation reasonably require additional time. Where Grantee, after reasonable efforts, is unable to identify an Affected Party, or receives no response from the Affected Party within thirty (30) days of Grantee's initial report, the ninety (90) day period runs from the date of Grantee's first reasonable attempt to make contact, and Grantee shall notify the Initiative before making any public disclosure on that basis. If Grantee has a good-faith belief that a vulnerability is being actively exploited, Grantee may accelerate disclosure to the extent reasonably necessary to protect users, but shall first make reasonable efforts to coordinate the timing and content of the disclosure with the Affected Party and shall concurrently notify the Initiative. Any public disclosure under this subsection shall be limited in content and manner to what is reasonably calculated to enable users and operators to protect themselves.

(4) Confidential Handling. Until public disclosure is permitted under subsection (3), Grantee shall (a) hold all vulnerability information, proof-of-concept code, and exploit artifacts in strict confidence and protect them with reasonable technical and organizational safeguards, including encryption in transit and at rest; (b) limit access to personnel with a need to know; (c) not share vulnerability information with any person other than the Affected Party and, as provided in subsection (6), the Initiative; and (d) not use, or permit the use of, any vulnerability for any purpose other than verification, remediation, and coordinated disclosure under this Section. Grantee shall not sell, license, or otherwise transfer any vulnerability, exploit, or related information to any person, including any exploit broker or acquisition program, except that Grantee may accept a bounty or reward from a program operated by or on behalf of the Affected Party. Grantee shall not trade in, or advise or enable any other person to

trade in, any digital asset or security on the basis of material nonpublic vulnerability information.

(5) Red-Teaming and AI-Assisted Testing. Where Grantee's project involves deliberate security or vulnerability testing using large language models or other artificial intelligence systems, Grantee shall (a) before commencing such testing, provide the Initiative with a written scope of engagement describing the intended targets, methods, model usage, and safeguards, which shall be deemed part of Grantee's proposal for purposes of Section A; (b) use such models and systems in accordance with the applicable model provider's terms of service and usage policies; (c) treat model inputs and outputs containing vulnerability information as confidential in accordance with subsection (4); (d) maintain human oversight of any agentic or autonomous testing and confine such testing to the environments and targets authorized under subsection (1); and (e) report any material vulnerability or dangerous capability identified in the artificial intelligence system itself to the model provider through the provider's designated disclosure channel.

(6) Notice to the Initiative. Grantee shall notify the Initiative in writing within ten (10) days of identifying a material vulnerability. Such notice shall be in summary form and shall not include vulnerability details, proof-of-concept or exploit code, or other information sufficient to enable exploitation. Grantee shall keep the Initiative reasonably informed of the status of coordination, remediation, and disclosure. The Initiative may request such further information as is reasonably necessary to verify Grantee's compliance with this Section, provided that Grantee shall not be required to provide, and the Initiative shall not require, information sufficient to enable exploitation of an unremediated vulnerability. The Initiative shall hold all information received under this Section in confidence until public disclosure is permitted under subsection (3).

(7) Publication. Following completion of coordinated disclosure under this Section, Grantee is encouraged to publish its research, methods, and findings in accordance with Section C.

(8) Breach. Any failure to comply with this Section constitutes a material breach of this Agreement and grounds for the Initiative to suspend, modify, or terminate the Grant under Section E and to require the return of Grant funds under Section F.

(9) Ownership of Security Findings. The Initiative does not acquire, solely by reason of making the Grant, any ownership, intellectual property, possessory, or other proprietary right in any vulnerability, exploit, proof of concept, security finding, research result, or related information discovered, developed, or obtained by Grantee through Grant-funded work. Nothing in this Agreement requires Grantee to provide the Initiative with vulnerability details, exploit or proof-of-concept code, credentials, keys, or other information sufficient to enable exploitation of an unremediated vulnerability. For avoidance of doubt, this subsection does not limit Grantee's

obligations under Section C following completion of the coordinated disclosure process described in this Section I.

J. Grantee shall indemnify, defend, and hold harmless the Initiative and its directors, officers, employees, and agents from and against any claim, demand, loss, liability, damage, cost, or expense (including reasonable attorneys' fees) arising out of or relating to Grantee's conduct of the project, Grantee's use of Grant funds, or any breach of this Agreement, except to the extent arising from the gross negligence or willful misconduct of the Initiative. Grantee is an independent grantee and is not an employee, agent, partner, or joint venturer of the Initiative, and nothing in this Agreement authorizes Grantee to act on the Initiative's behalf or to bind the Initiative. The Initiative does not direct, supervise, or control Grantee's activities, including any security research or testing conducted under Section I, and the award of the Grant does not constitute authorization by the Initiative or by any third party for Grantee to access, test, or otherwise interact with any system. Sections I and J survive the expiration or termination of this Agreement.

K. This Agreement shall be governed by the laws of the State of Texas. Any dispute over the terms of this Agreement and the actions of the parties under this agreement shall take place in the State and Federal courts located in Travis County, Texas.

Grantee accepts responsibility for complying with this agreement's terms and conditions and will exercise full control over the grant and the expenditure of grant funds. This grant will be payable according to the above referenced payment schedule, after the Initiative receives a copy of this agreement signed by an authorized officer of Grantee. Grantee may wish to have this agreement reviewed by legal counsel.

[Signature Page Follows]

On behalf of Grantee, I understand and agree to the foregoing terms and conditions of the Initiative's grant, and hereby certify my authority to execute this agreement on Grantee's behalf.

GRANTEE	**OPEN SATS INITIATIVE, INC**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Exhibit A

Grant Proposal