ZCG Security & Vulnerability Disclosure Initiative

Terms of Participation

Version 1.0 — April 27, 2026

> *These Terms of Participation ("Terms") govern all submissions made to the ZCG Security & Vulnerability Disclosure Initiative ("Program"). By submitting a vulnerability report under the Program, a researcher agrees to be bound by these Terms. No registration or prior acceptance is required; submission constitutes agreement.*

1. Parties and Administration

The Program is operated by Zcash Community Grants ("ZCG"), with administrative support provided by the Financial Privacy Foundation ("FPF") pursuant to FPF's existing support agreement with ZCG. References to "ZCG" in these Terms include FPF acting in its administrative capacity on ZCG's behalf.

The "remediation team" for any given disclosure is the group of engineers drawn from the affected core ecosystem projects (which may include ZODL, ZF, Shielded Labs, and/or other repository owners) who triage, grade, and coordinate remediation of that disclosure. Composition varies by disclosure. The remediation team is not a party to these Terms; rather, it operates within the Program's framework as described in the main Program announcement.

2. Definitions

- "Acknowledgment" means written confirmation by the remediation team that a Submission has been received and is under review.
- "Disclosure" means any communication by a Researcher to the remediation team describing a potential vulnerability.
- "Embargo Period" has the meaning given in Section 5.1.
- "Patch Release" means the public availability of a fix for a vulnerability addressed by a Disclosure.
- "Program" means the ZCG Security & Vulnerability Disclosure Initiative as described in the Program Announcement and these Terms.
- "Program Announcement" means ZCG's public announcement of this Program, as published on the Zcash Community Forum.
- "Researcher" means any individual or organization that submits a Disclosure under the Program.
- "Submission" means the complete package of materials a Researcher delivers in connection with a Disclosure, including any report, proof-of-concept, reproduction steps, and supporting materials.

3. Researcher Representations and Warranties

By submitting a Disclosure, the Researcher represents and warrants to ZCG that, as of the date of submission and as of any payout date:

3.1 Independence and Eligibility

- The Researcher is not currently employed by, contracted by, or otherwise engaged as a paid contributor to ZODL, ZF, Shielded Labs, Zingolabs, or Least Authority Enterprises on Zcash core or core-adjacent repositories (including Zaino and Zallet), and will promptly notify the remediation team if that status changes during an active disclosure cycle.
- The Researcher's discovery arose from independent security research and not from access to non-public information obtained through any employment, contract, or confidential relationship.
- The Researcher is not a person or entity subject to applicable sanctions, including those administered by the U.S. Office of Foreign Assets Control (OFAC), the EU, or the UN Security Council, and is not located in or ordinarily resident in a jurisdiction subject to comprehensive sanctions.

3.2 Prior Conduct

- The Researcher has not previously exploited the disclosed vulnerability, in whole or in part, on mainnet, testnet, or any production infrastructure.
- The Researcher has not shared the vulnerability, or any material details sufficient to enable exploitation, with any third party prior to or during the Embargo Period, except as expressly permitted under Section 5.
- The Researcher has not used knowledge of the vulnerability to acquire, dispose of, or otherwise trade ZEC or any instrument whose value is materially affected by the vulnerability.

3.3 Ownership

- The Submission is the Researcher's original work. The Researcher has not assigned, licensed, or otherwise encumbered the intellectual property in the Submission in a way that would prevent the remediation team from using it for remediation purposes.
- Where the Researcher is employed, the Researcher has confirmed that their employer's IP assignment policy does not cover the Submission, or has obtained appropriate written authorization.

4. Researcher Obligations

4.1 Responsible Disclosure Channel

Researchers must submit Disclosures through the responsible-disclosure channel specified in the SECURITY.md file of the most relevant in-scope repository. ZCG and

FPF do not accept Disclosures through any channel and must not be contacted with vulnerability details. Disclosures sent to ZCG or FPF will not be triaged and will not establish eligibility for a payout.

4.2 Scope of Research

- Researchers must limit their testing to the minimum necessary to confirm and characterize the vulnerability. Continued probing beyond what is necessary to establish reproducibility and severity is not permitted.
- Researchers must not access, exfiltrate, copy, or retain any data encountered incidentally during research that does not belong to them.
- Researchers must not pivot from an in-scope repository or system to any out-of-scope system, even if a technical path to do so exists.
- Automated scanning and fuzzing must be conducted in isolated environments (local testnet, regtest, or equivalent). Automated tools must not be directed at production infrastructure or public testnets in a manner that degrades availability for other users.
- Researchers must not conduct social engineering, phishing, or physical security attacks against any individual or organization in connection with their research.

4.3 Responsiveness

Researchers are expected to respond to requests from the remediation team within five (5) business days. Failure to respond within this window may result in the Submission being deprioritized and may affect bonus eligibility, at the discretion of the remediation team. It will not by itself affect base payout eligibility for a finding that has already been categorized and graded.

4.4 Conduct During Triage

- Researchers must engage professionally and in good faith throughout the triage and remediation process.
- Researchers must not make public statements about an active Disclosure while the Embargo Period is in effect, including statements that imply the existence of an undisclosed vulnerability without providing technical details.
- Researchers must not use the existence of an active Disclosure as leverage in any negotiation with ZCG, FPF, or any core ecosystem organization.

5. Embargo and Coordinated Disclosure

5.1 Embargo Period

From the date of Acknowledgment, a Researcher agrees not to publicly disclose any details of the Disclosure (“Embargo Period”) until the earliest of:

- the Patch Release has been made publicly available and the remediation team has confirmed that a coordinated public disclosure may proceed;

- ninety (90) calendar days after Acknowledgment, subject to Section 5.3 (Extension); or
- a Forced Disclosure event as described in Section 5.4.

The Embargo Period applies to all forms of public communication, including but not limited to: blog posts, forum posts, social media, conference presentations, academic papers, CVE database submissions, and conversations with third parties not directly involved in remediation.

5.2 Clock and Acknowledgment

The Embargo Period clock begins on the date the remediation team sends written Acknowledgment. If a Researcher does not receive Acknowledgment within ten (10) business days of submitting a Disclosure, the Researcher may request confirmation of receipt directly from the repository maintainer via the channel specified in the applicable SECURITY.md. The absence of Acknowledgment does not suspend the Researcher's obligations under Section 4.

5.3 Extension by Mutual Agreement

The remediation team and the Researcher may agree in writing to extend the Embargo Period beyond ninety (90) days where active remediation work is ongoing and an extension is reasonably necessary to protect users. Extensions should be memorialized by written agreement between the Researcher and the remediation team and should specify a revised target date. No single extension may exceed sixty (60) additional days without the Researcher's renewed written consent.

5.4 Forced Disclosure (Dead Man's Switch)

If the remediation team has not provided a credible patch timeline within thirty (30) calendar days of Acknowledgment, or if a patch has not been deployed within ninety (90) calendar days of Acknowledgment (absent a written extension under Section 5.3), the Researcher may disclose the vulnerability publicly after providing the remediation team with seven (7) calendar days' prior written notice of their intent to do so. This right exists to protect researchers from indefinite embargo and does not affect payout eligibility for a finding that has been categorized and graded.

This provision does not apply where the remediation team can demonstrate, in writing, that active remediation work is ongoing and that disclosure would cause immediate, material harm to users. In such cases the parties must negotiate in good faith toward a mutually acceptable disclosure date.

5.5 Independent Discovery

If a Researcher becomes aware, during the Embargo Period, that the same vulnerability has been independently discovered by a third party or is being actively exploited in the wild, the Researcher must notify the remediation team promptly. This notification may accelerate the coordinated disclosure timeline at the remediation team's discretion.

5.6 Post-Embargo Publication

After the Embargo Period ends and the Patch Release has been made, Researchers are encouraged to publish write-ups describing their work. Pre-publication review by the remediation team is strongly encouraged to avoid inadvertent residual disclosure of sensitive implementation details. The remediation team will complete any requested review within thirty (30) calendar days of receiving a draft.

6. Prohibited Conduct

The following conduct is prohibited at all times, including before, during, and after an active disclosure cycle. Engaging in prohibited conduct will result in forfeiture of all payout eligibility and may result in legal referral:

- Exploiting a vulnerability on mainnet or any production infrastructure for any purpose, including proof-of-concept demonstration.
- Using knowledge of a vulnerability to trade ZEC or any instrument whose value is materially affected by the vulnerability (“insider trading analog”).
- Sharing, selling, brokering, or otherwise transferring a vulnerability or any material details sufficient to enable exploitation to any third party, including other researchers, exchanges, mining pools, or market participants, before or during the Embargo Period.
- Conducting denial-of-service attacks, network floods, or other disruptive actions against any node, wallet, or infrastructure, beyond what is narrowly necessary to confirm a finding in an isolated environment.
- Accessing, exfiltrating, or retaining user data, private keys, seeds, or any data belonging to third parties encountered during research.
- Fabricating, inflating, or artificially escalating the severity of a finding.

7. Payment Terms

7.1 Payment Process

Payments are initiated by the remediation team, not by Researchers. Once a Disclosure has been triaged, remediated, and categorized, the remediation team submits a payment request to ZCG on the Researcher’s behalf. Researchers must not invoice ZCG, FPF, or any core ecosystem organization directly.

7.2 Currency and Conversion

Payout amounts are denominated in USD. Payment will be made in shielded ZEC. The ZEC amount will be calculated using the USD/ZEC spot price at the time FPF initiates the transaction, as sourced from a reputable exchange or aggregator selected by FPF at its discretion. FPF bears no responsibility for price movements between approval and execution.

7.3 KYC Requirements

Payouts exceeding $50,000 USD in aggregate per Researcher per calendar year require completion of KYC verification administered by FPF. FPF will initiate the KYC process upon approval of a qualifying payment request. Payment will be held pending KYC completion and will be released within fifteen (15) business days of successful verification.

7.4 OFAC and Sanctions Screening

All payouts are subject to OFAC and equivalent sanctions screening. Payment will not be made to any person, entity, or jurisdiction subject to applicable sanctions. Where a Researcher fails sanctions screening, ZCG will notify the Researcher and no payout will be issued. Researchers are responsible for the accuracy of their representations under Section 3.1.

7.5 Pool Exhaustion

ZCG has earmarked $1,000,000 USD for this Program. In the event the pool is exhausted or materially depleted, ZCG will post a public notice on the Zcash Community Forum. Submissions received before the pool exhaustion notice is posted that are subsequently categorized and graded as eligible will be honored to the extent funds remain available, in order of remediation team payment request submission. Submissions received after a pool exhaustion notice has been posted will not be eligible for payout unless ZCG announces additional funding.

7.6 Taxes

Researchers are solely responsible for all tax obligations arising from payments received under this Program. ZCG and FPF make no representations regarding the tax treatment of any payout. Researchers in jurisdictions requiring withholding may be asked to provide applicable tax documentation before payment is released.

8. Intellectual Property

8.1 License to Submission

By submitting a Disclosure, the Researcher grants ZCG, FPF, and the remediation team a non-exclusive, worldwide, royalty-free license to use, reproduce, and modify the Submission (including any proof-of-concept code, test cases, and supporting materials) solely for the purpose of remediating the disclosed vulnerability and hardening the affected software. This license does not transfer ownership of the Submission to ZCG or any third party.

8.2 Researcher Ownership

The Researcher retains ownership of the Submission and, following expiration of the Embargo Period, may publish write-ups, present at conferences, and otherwise publicly describe their research, subject to Section 5.6.

8.3 No Obligation to Open-Source

Nothing in these Terms requires the Researcher to open-source any tooling, scripts, or code developed in connection with their research.

9. Confidentiality

Each Researcher agrees to treat all non-public technical details of an active Disclosure as confidential during the Embargo Period. This obligation survives the expiration of these Terms with respect to any specific finding until that finding has been publicly disclosed by the remediation team or the Embargo Period has ended under Section 5.

ZCG and FPF will not receive or retain technical vulnerability details as part of the payment process. The remediation team is responsible for handling technical information in accordance with the applicable SECURITY.md and its own disclosure practices.

10. Limitation of Liability and Dispute Resolution

10.1 No Dispute Process

As described in the Program Announcement, ZCG does not manage, respond to, or resolve disputes between Researchers, organizations, and remediation teams. Disputes regarding severity categorization, base payout amounts, or bonus determinations are a matter for the Researcher and the remediation team.

Bonus determinations are final and are not subject to any dispute or appeal process.

10.2 Good Faith Escalation

Where a Researcher believes a base payout determination is inconsistent with the published payout schedule or these Terms, the Researcher may raise the matter with ZCG in writing, identifying the specific inconsistency. ZCG will review the payment request for consistency with the Program and may request clarification from the remediation team. ZCG’s determination following such review is final.

10.3 Limitation of Liability

To the maximum extent permitted by applicable law, neither ZCG nor FPF shall have any liability to any Researcher arising out of or in connection with this Program. This exclusion applies to all claims and theories of liability, including contract, tort, and statute, except that nothing in this section limits liability for ZCG's or FPF's own fraud or willful misconduct.

10.4 Governing Law

These Terms are governed by the laws of The Cayman Islands, without regard to its conflict of laws principles. Any dispute that is not resolved informally shall be subject to the exclusive jurisdiction of The Cayman Islands.

11. General Provisions

11.1 Entire Agreement

These Terms, together with the Program Announcement, constitute the entire agreement between ZCG and each Researcher with respect to the Program and supersede all prior understandings, representations, and communications relating to the same subject matter.

11.2 Amendment

FPF may amend these Terms by posting a revised version on the Zcash Community Forum. Amendments will not apply retroactively to Disclosures for which Acknowledgment has already been issued; the Terms in effect at the time of Acknowledgment govern that disclosure cycle.

11.3 Severability

If any provision of these Terms is held invalid or unenforceable, that provision will be limited to the minimum extent necessary, and the remaining provisions will continue in full force and effect.

11.4 No Waiver

ZCG's failure to enforce any provision of these Terms on one occasion does not waive its right to enforce that provision on any other occasion.

11.5 Relationship of Parties

Researchers are independent parties. Nothing in these Terms creates an employment, agency, partnership, or joint venture relationship between any Researcher and ZCG, FPF, or any core ecosystem organization.

11.6 No Registration Required

There is no sign-up or pre-approval step for this Program. Attempting to register with ZCG or FPF does not establish eligibility. Eligibility is determined solely by the Program Announcement criteria and these Terms, applied at the time a payment request is reviewed.

Appendix A follows on the next page.

Appendix A: Large Payout Signature Addendum

> *This Addendum applies only to Submissions where the proposed total payout (base plus bonus) equals or exceeds $50,000 USD. For all other Submissions, the Terms of Participation govern without any separate signature requirement.*

This Signature Addendum (“Addendum”) is entered into between Financial Privacy Foundation (FPF), administrators of the Zcash Community Grants (ZCG) program, and the undersigned Researcher, and is incorporated into and forms part of the Terms of Participation for the ZCG Security & Vulnerability Disclosure Initiative.

By signing below, the Researcher confirms that:

- They have read, understood, and agreed to the Terms of Participation in their entirety.
- All representations and warranties in Section 3 are true and accurate as of the date of signature.
- They consent to KYC verification by FPF as a condition of receiving payment.
- They acknowledge the governing law and jurisdiction provisions of Section 10.4.
- For payouts to an entity rather than an individual: the signatory has authority to bind the entity, and the entity’s KYC documentation will include proof of that authority.

Researcher / Authorized Signatory:

Signature: _____

Printed Name: _____

Title (if signing on behalf of entity):

_____

Entity Name (if applicable): _____

Date: _____

Shielded ZEC Address: _____

For FPF:

Signature: _____

Printed Name: _____

Title: _____

Date: _____