**Responsible Disclosure Policy**

## Purpose

To allow for the reporting and disclosure of vulnerabilities discovered by external personnel and entities.  This policy does not apply to Hashgraph employees and contractors.

## Scope

Hashgraph’s Responsible Disclosure Policy applies to Hashgraph’s core platform and its information security infrastructure or third parties.

## Background

Hashgraph is committed to ensuring the safety and security of our customers. We aim to foster an environment of trust, and an open partnership with the security community, and we recognize the importance of vulnerability reporting and disclosures in continuing to ensure safety and security for all of our customers, employees and company. We have developed this policy to both reflect our corporate values and to uphold our responsibility to good-faith security researchers that are providing us with their expertise and reporters of potential vulnerabilities who contribute an extra layer of security to our infrastructure.

## Posture

Subject to the conditions below, Hashgraph will not engage in legal action against individuals for submitting vulnerability reports through our Vulnerability Reporting inbox. We openly accept reports for Hashgraph products. To encourage the discovery and reporting of vulnerabilities, we agree not to pursue legal action against individuals based on the individual:

- Engaging in testing of systems/research without harming Hashgraph or its customers.
- Engaging in vulnerability testing within the scope of our Vulnerability Disclosure Program, as detailed below.
- Adhering to the laws of their location and the location of Hashgraph. For example, violating laws that would only result in a claim by Hashgraph (and not a criminal claim) may be acceptable as Hashgraph is authorizing the activity (reverse engineering or circumventing protective measures) to improve its system.
- Perform testing only on your own accounts and systems, and avoid actions that

could disrupt our services or compromise data.

- Never attempt non-technical attacks. Social engineering, phishing, or physical attacks against anyone, including but not limited to Hashgraph employees, contractors, node operators, developers, or users, or against the network infrastructure is not allowed.
- Avoid Public Disclosure:
    - Do not publicly disclose the vulnerability until we have had a reasonable opportunity to address it.
- Respect Privacy:
    - Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during your research.

## Policy

### Submitting a Report

***How to Submit a Vulnerability***

To submit a vulnerability report to Hashgraph's Product Security Team, please utilize the following email: security@hashgraph.com.

***Preference, Prioritization, and Acceptance Criteria***

We will use the criteria from the next sections to prioritize and triage submissions.

***What we would like to see from you:***

- Well-written reports in English will have a higher probability of resolution.
- Reports that include proof-of-concept code equip us to better triage.
- Reports that include only crash dumps or other automated tool output may receive lower priority.
- Reports that include products not on the initial scope list may receive lower priority.
- Please include how you found the bug, the impact, and any potential remediation.

***What you can expect from Hashgraph:***

- A timely response to your email (within 5 business days).
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it.
- An open dialog to discuss issues.

- Notification when the vulnerability analysis has completed each stage of our review.

If we are unable to resolve communication issues or other problems, Hashgraph may, in its sole discretion, bring in a neutral third party to assist in determining how best to handle the vulnerability.

**Legal Safe Harbor**

Hashgraph will not take legal action against individuals who report vulnerabilities responsibly and in full compliance with this policy. We consider vulnerability disclosure activities conducted in accordance with this policy as authorized conduct and exempt from any breach of applicable anti-hacking obligations.