ANTIGRAVITY

Product Security Vulnerability Disclosure Policy

Last Updated: July 24, 2026

1. Introduction

We are committed to protecting our customers' security and privacy. This policy is intended to provide security researchers and the public with a clear channel and guidelines for responsibly reporting potential security vulnerabilities in the electronic products we sell. We are committed to complying with vulnerability disclosure regulations in all countries and to coordinating transparently and in good faith with reporters.
We recommend that you read this policy in its entirety before submitting a vulnerability report, and always adhere to it. We value everyone who invests time and effort in reporting security vulnerabilities in accordance with this policy. Please note, however, that we do not offer monetary rewards for vulnerability disclosure.

2. How to Report a Security Vulnerability

If you discover a potential security vulnerability in any of our electronic products (including hardware devices, firmware, companion apps, or cloud services), please contact us through the dedicated channel below:
Email: service@antigravity.tech
Important: To protect users, please do not publicly disclose any details before the vulnerability is fixed. Do not engage in any exploitation that could damage device functionality, user data, or service availability without communicating with us and obtaining our consent.

3. Information that Helps Us Respond Faster

Please provide as much of the following information as possible in your report. This will help us accelerate the assessment and remediation process:

Information Item	Details
Affected Product	
Software/Firmware Version	
Vulnerability Description	
Impact Assessment	
Contact Information （optional）	

4. Vulnerability Report Response

4.1 Acknowledgment Timeframe

We commit to sending an initial acknowledgment within 48 hours (within two business days) of receiving a report, confirming receipt and informing you of the current processing status.

4.2 Processing Status and Timeframes

We will assess and remediate vulnerabilities based on their severity and exploitability. General timeframes are as follows:

Processing Stage	Estimated Time (Business Days)	Description
Initial Assessment	5 days	Validate the vulnerability and determine its severity level.
Fix Development	15 to 30 days	Time may vary depending on complexity.
Internal Testing & Preparation	5 to 10 days	Ensure the fix does not affect normal product functionality.
Update Rollout	Per product update cycle	Delivered in the next scheduled security update for remotely updatable products. For devices requiring manual updates, we will issue an advisory and provide tools.

4.3 Coordinated Disclosure Commitment

Good-Faith Protection: We will not pursue legal action against security researchers who act in good faith and comply with this policy. We consider you a partner in protecting our customers.

No Unauthorized Disclosure: We will not unilaterally disclose the technical details of a vulnerability before a patch or mitigation is fully deployed to users.

Coordinated Disclosure: We are willing to work with you to agree on a mutual public disclosure date (typically no later than 30 days after the fix becomes available), ensuring users have sufficient time to upgrade while your discovery receives proper recognition.

acknowledgement: With your consent, we will recognize your contribution in our public security advisories, acknowledgement pages, or release notes.

4.4 Our Expectations

We kindly request that reporters:

1) Keep vulnerability information strictly confidential until the agreed disclosure date.

2) Refrain from any data access, modification, or deletion beyond what is necessary for proof of concept.
3) Do not disclose vulnerability information to any third party in any way, unless legally compelled.
4) Report the vulnerability through the channel provided in this policy immediately upon discovery, rather than exploiting it for improper gain.

5. Important Notes

While we encourage the investigation of potential security vulnerabilities, we cannot tolerate any activity that may disrupt legitimate users or violate applicable computer misuse, cybersecurity, and data protection laws. Therefore, the following activities are prohibited:

- Service disruption or degradation, such as Denial of Service (DoS)
- Disclosure of personal information, proprietary information, or financial information
- Violation of any applicable laws or regulations
- Accessing unnecessary, excessive, or bulk amounts of data
- Tampering with data in our organization's systems or services
- Using highly intrusive or destructive scanning tools to probe for vulnerabilities
- Interfering with the operation of our organization's services or systems

6. **Security Update Support Period**

We strive to provide ongoing security updates for our products. Security updates typically include the latest patches, vulnerability fixes, and other security improvements. We generally maintain security updates for at least 2 years from the product launch date. However, security update support periods may vary by product; please follow our announcements.

We periodically publish and update information regarding the security of ANTIGRAVITY products on this page to help you check for security updates for your device.

product type	product name	Model	Launch Date	Security Update End Date
drone	Antigravity A1	DE001，DE001B	2025/12/31	2028/12/31
Vision Goggles	Antigravity Vision	DGS001	2025/12/31	2028/12/31