TRUST AND SECURITY

Security and Vulnerability Disclosure Policy

How we protect the Service, what security testing is permitted, how to report a vulnerability, and our commitment not to pursue good-faith researchers.

Version 1.0 - Effective 29 August 2026 - Updated 29 August 2026 - 8 sections - 55 clauses

Document ref. WGN-LEGAL-SECURITY-V1.0

Published by Lacspace Corporation Pvt. Ltd. (Nepal reg. 377566/82/83; India CIN U46511DL2025PTC079972), Bhimsengola, Sinamangal, Kathmandu, Bagmati Province, Nepal. This file is a controlled copy provided for reference; the version published at the address below is authoritative.
ideatopic.com/legal/security

CONTROLLED COPY
WGN-LEGAL-SECURITY-V1.0

AT A GLANCE

A plain-language summary. The numbered clauses below are what legally applies.

- Report anything you find to security@lacspace.com. We reply within 3 working days.
- We will not pursue legal action against good-faith research within the stated rules.
- Do not access other people's data, degrade the Service, or use social engineering.
- We have no paid bug bounty, but we credit reporters who want it.
- A breach affecting users is disclosed within 72 hours.

1. Our commitments

1.1 Traffic between your device and the Service is encrypted in transit using TLS.

1.2 Passwords are stored only as salted cryptographic hashes and are never recoverable.

1.3 Data at rest is encrypted by our storage providers.

1.4 Access to production systems and data is restricted to personnel who require it, and is logged.

1.5 Authentication endpoints are rate limited and monitored for automated abuse.

1.6 Sessions expire and tokens are rotated.

1.7 Dependencies are monitored for known vulnerabilities and updated.

1.8 We do not claim the Service is perfectly secure. No system is, and a claim to the contrary would be worthless.

2. Reporting a vulnerability

2.1 Send reports to security@lacspace.com with "Vulnerability" in the subject line.

2.2 Include the affected URL or endpoint, the steps to reproduce, and the impact you believe it has.

2.3 Include a proof of concept where you can do so without accessing another person's data.

2.4 We acknowledge every report within three working days.

2.5 We give an initial assessment within ten working days.

2.6 We keep you informed while we work on a fix, and we tell you when it is deployed.

2.7 We ask that you do not disclose publicly until a fix is deployed, or ninety days have passed, whichever is sooner.

2.8 You do not need an account to report, and we accept anonymous reports.

3. Safe harbour

3.1 We will not bring or support legal proceedings against a person conducting security research in good faith within the rules in this policy.

> *A disclosure policy without this commitment is a trap. Researchers are asked to identify themselves and describe exactly what they did, and they need to know that will not be used against them.*

3.2 We will not report good-faith research to law enforcement.

3.3 We consider such research authorised access for the purposes of any law restricting unauthorised access.

3.4 If a third party brings proceedings in respect of research conducted within these rules, we will make clear that it was authorised.

3.5 Safe harbour is lost if you access, copy or retain another person's data, degrade the Service, extort us, or disclose in breach of the timescales above.

3.6 If you are unsure whether an action is within scope, ask before you take it.

4. Permitted testing

4.1 Testing against your own account and your own content.

4.2 Passive observation of responses, headers and client-side code.

4.3 Testing for injection, authentication, authorisation and access-control flaws using your own data.

4.4 Reporting misconfiguration of storage, headers, certificates or DNS.

4.5 Reporting a dependency with a known vulnerability.

4.6 Testing that stops at the first proof that a flaw exists.

5. Prohibited testing

5.1 Accessing, downloading, modifying or retaining any data belonging to another person.

5.2 Denial of service testing, load testing, or anything that degrades the Service for other users.

5.3 Social engineering of our staff, our users, our contractors or our suppliers.

5.4 Physical attacks on any premises or equipment.

5.5 Spam, phishing or any test conducted against a third party's system.

5.6 Automated scanning that generates a volume of traffic capable of affecting availability.

5.7 Retaining a copy of anything you obtained during testing after you have reported it.

CONTROLLED COPY WGN-LEGAL-SECURITY-V1.0

(c) 2026 Lacspace Corporation Pvt. Ltd. - IdeaTopic is a product of Lacspace.
Controlled copy. Authoritative version: ideatopic.com/legal/security

5.8 Publishing details of an unfixed vulnerability.

6. Out of scope

6.1 Reports produced solely by an automated scanner without a demonstrated impact.

6.2 Missing security headers with no demonstrated exploit.

6.3 Weaknesses in third-party services we do not control.

6.4 Issues requiring physical access to an unlocked device.

6.5 Self-inflicted issues requiring the victim to paste code into a console.

6.6 Best-practice recommendations without a security impact.

6.7 Rate limiting on endpoints where a limit exists and functions.

7. Recognition

7.1 We do not operate a paid bug bounty programme, and we say so rather than implying one.

7.2 We credit reporters publicly where they wish to be credited.

7.3 We will provide a written acknowledgement of a valid report on request.

7.4 We prioritise fixing over negotiating about severity.

7.5 A report that leads to a material fix is acknowledged in the relevant version history.

8. If a breach occurs

8.1 We investigate immediately and take steps to contain the incident.

8.2 Where a breach is likely to result in a risk to users, we notify affected users and the relevant authority without undue delay, and in any event within seventy-two hours of becoming aware of it.

8.3 A notification states what happened, what data was involved, what we have done, and what you should do.

8.4 We do not delay notification in order to complete an investigation first.

8.5 We publish a post-incident account where doing so does not create further risk.

8.6 We preserve incident records for at least five years.

8.7 We do not retaliate against a person who reported the issue that led to the discovery.

Version history

v1.0 - 29 August 2026

- Initial publication.
- Added an express safe harbour commitment with defined limits.
- Published scope, permitted testing and out-of-scope categories.
- Stated plainly that there is no paid bounty programme.

CONTROLLED COPY WGN-LEGAL-SECURITY-V1.0

Publisher, contact and document control

Lacspace Corporation Pvt. Ltd.
IdeaTopic is a product of Lacspace.

Registration	Nepal 377566/82/83 - India CIN U46511DL2025PTC079972
Registered office	Bhimsengola, Sinamangal, Kathmandu, Bagmati Province, Nepal
Telephone	+977 9705 300600
General enquiries	hello@lacspace.com
Legal notice	legal@lacspace.com
Abuse and safety	abuse@lacspace.com
Security disclosure	security@lacspace.com
This document	ideatopic.com/legal/security
Legal Centre	ideatopic.com/legal
Product	ideatopic.com
Publisher	lacspace.com
Document reference	**WGN-LEGAL-SECURITY-V1.0**
Version	1.0, effective 29 August 2026 (last updated 29 August 2026)
Governing law	This document is governed by the laws of Nepal, with the courts of Kathmandu, Nepal having jurisdiction.

This is a controlled copy. The version published at ideatopic.com/legal/security governs, and supersedes this file the moment a new version is issued there. A printed or forwarded copy is uncontrolled: check the reference and version above against the web version before relying on it. (c) 2026 Lacspace Corporation Pvt. Ltd. All rights reserved.

CONTROLLED COPY
WGN-LEGAL-SECURITY