Scan for the live version

TRUST & SAFETY

Responsible Disclosure

How to report a security vulnerability to us safely, and what you can expect in return.

VERSION	v1.0
EFFECTIVE DATE	10 August 2026
LAST UPDATED	10 August 2026
CLASSIFICATION	Public
STRUCTURE	12 sections - 31 clauses
DOCUMENT ID	SY-LEGAL-RESPONSIBLE-DISCLOSURE-V1.0
GOVERNING LAW	Laws of Nepal - Courts of Kathmandu
ISSUED BY	Lacspace - Legal & Compliance

AT A GLANCE

- Found a security issue? Email security@stockyatra.com with clear steps to reproduce.
- Good-faith research that follows this policy gets our safe harbour - we won't pursue legal action.
- Don't access other users' data, disrupt the Service, or disclose publicly before we've fixed it.
- StockYatra holds no client securities and simulates trading, so no real money is at risk - but we take every report seriously.
- We acknowledge, triage, remediate and keep you updated, and we'll credit you if you wish.

Contents

1. Purpose & Our Commitment to Security
2. Scope
3. Safe Harbour
4. How to Report
5. What We Ask You NOT to Do
6. Our Response Process
7. Coordinated Disclosure
8. Recognition
9. No Compromise of User Data or Real Money
10. Legal & Good Faith
11. Changes to This Policy
12. Contact

1. Purpose & Our Commitment to Security

This Responsible Disclosure Policy explains how to tell us about a security vulnerability, and how we will respond. It should be read together with our Acceptable Use Policy and Terms of Use.

1.1 StockYatra is an educational paper-trading simulator built in Nepal by Lacspace Corporation Pvt. Ltd. We care about protecting our learners, their accounts and their personal data, and we welcome the help of the security-research community in keeping the Service safe.

1.2 "The Service" means the StockYatra website, our mobile apps, and our public API. "You" means any individual who researches or reports a security issue to us under this policy.

1.3 If you believe you have found a vulnerability, we want to hear from you. This policy tells you what we consider fair game, how to report responsibly, and what we commit to in return.

2. Scope

This policy covers vulnerabilities in the systems we own and operate. The following are in scope:

2.1 In scope:

a. the StockYatra website and its public web application;
b. our official StockYatra mobile apps for Android and iOS;
c. our public API used by the website and apps.

2.2 Out of scope. The following are not covered by this policy, and testing them is not authorised:

a. third-party services we do not control, including our hosting, analytics, email and payment providers, and their infrastructure;
b. social engineering, phishing or any attempt to deceive our staff, contractors or users;
c. physical attacks against our people, offices or hardware;
d. denial-of-service, volumetric, load or stress testing of any kind;
e. automated scanner output submitted without a demonstrated, exploitable impact.

2.3 If you are unsure whether a target or technique is in scope, ask us first at security@stockyatra.com before you test.

3. Safe Harbour

3.1 We will not pursue or support legal action against you for security research carried out in good faith that follows this policy. We consider such research to be authorised, and we will not treat it as a breach of our Acceptable Use Policy or Terms of Use.

3.2 "Good faith" means you make a sincere effort to avoid harm to users, data and the Service, you stay within the scope above, you do only what is necessary to demonstrate the issue, and you report it to us promptly and privately.

3.3 This safe harbour does not apply to activity that is unlawful, that falls outside the scope of this policy, or that continues after we have asked you to stop. It also cannot bind third parties - if your testing affects a service we do not control, their terms and the law still apply.

4. How to Report

Send your report to security@stockyatra.com. To help us act quickly, please include:

4.1 A clear, complete report containing:

a. clear, step-by-step instructions to reproduce the issue;
b. the affected URL, endpoint, app screen or component;
c. the impact - what an attacker could do, and to whom;
d. any proof-of-concept, request/response samples, logs or screenshots that help us validate it.

4.2 Please report one issue per email where you can, and use a descriptive subject line. If a finding is sensitive, you may ask us for a secure channel and we will arrange one.

4.3 Report a vulnerability as soon as you can after you find it, and give us a reasonable opportunity to investigate and fix it before you take any further action.

5. What We Ask You NOT to Do

To keep your research within safe harbour, please do not:

5.1 Access, modify, delete or exfiltrate data that does not belong to you, including any other user's account, personal data or virtual balances. If you accidentally encounter such data, stop, do not save or share it, and tell us in your report.

5.2 Degrade, disrupt or damage the Service, or interfere with the experience of other users - for example through denial-of-service, spam, or destructive testing.

5.3 Publicly disclose the vulnerability, or share it with anyone else, before we have fixed it and agreed the timing of any disclosure with you.

5.4 Break the law, or violate the privacy of our users or staff, in the course of your research. When in doubt, do less and ask us.

6. Our Response Process

When you report a vulnerability in good faith, we aim to work with you. On a best-effort basis - these timelines are targets, not guarantees:

6.1 Our process typically follows these steps:

a. acknowledge receipt of your report, usually within a few business days;
b. triage and validate the issue, and ask you for any further detail we need;
c. remediate confirmed vulnerabilities, prioritised by severity and risk to users;
d. keep you updated on progress, and let you know when the fix is live.

6.2 Timelines depend on the complexity and severity of the issue and on our resources as a small team. We will be honest with you about where things stand.

6.3 If we decide an issue is out of scope, is not a vulnerability, or is a duplicate of one already known to us, we will tell you and explain why.

7. Coordinated Disclosure

7.1 We support coordinated disclosure. Once a vulnerability is fixed, we will agree a disclosure timeline with you, so that any public write-up appears only after users are protected.

7.2 Please do not disclose details of the vulnerability publicly until we have confirmed the fix is deployed and we have agreed the timing with you. We will not unreasonably delay disclosure of a resolved issue.

8. Recognition

8.1 We are grateful to researchers who help us keep StockYatra safe. Where you would like it, and where your report led to a fix, we are happy to credit you by name or handle.

8.2 This is a voluntary programme. We do not operate a paid bug-bounty and do not guarantee any monetary reward or bounty for a report. Any recognition or thanks is at our discretion.

9. No Compromise of User Data or Real Money

9.1 StockYatra is an educational simulator. It executes no real trades and holds no client securities. Trading uses virtual money only, and in-app coins are an educational currency with no monetary value that cannot be withdrawn or redeemed for real money. See our Risk Disclaimer for more.

9.2 Because of this, a vulnerability in the Service cannot cause a loss of real securities or real client funds. Even so, we take every report seriously - the protection of user accounts and personal data matters to us regardless of the money model.

10. Legal & Good Faith

10.1 Your research must comply with all applicable laws, including the laws of Nepal and any laws that apply to you where you carry out your testing. Nothing in this policy authorises activity that is unlawful.

10.2 This policy does not grant you any right to access data or systems beyond what is reasonably necessary to identify and demonstrate a vulnerability within scope.

10.3 For how we handle any personal data contained in a report, see our Privacy Policy.

11. Changes to This Policy

11.1 We may update this policy from time to time. The current version is always the one published at stockyatra.com/legal/responsible-disclosure, and the effective date at the top reflects the latest revision.

11.2 Material changes will be notified through the Service or by other reasonable means. The version that applies to your report is the one in force when you submit it.

12. Contact

12.1 To report a security vulnerability: security@stockyatra.com. For other legal questions: legal@stockyatra.com.

This document is a professionally drafted template provided for transparency. It is not legal advice and should be reviewed by qualified counsel before you rely on it.