Tribepad

# Responsible Vulnerability Disclosure Program

# 1.0 Vulnerability disclosure program

We believe that security comes first and that white hat hackers play a vital role in strengthening the world's security posture.

If you believe that you have discovered a vulnerability then please disclose this to us by emailing security@tribepad.com. We will work with you to validate your submission and remediate the vulnerability as soon as possible.

Before you submit any vulnerabilities please review **all** the sections in this document.

## 1.1 Service level agreement

Please allow up to 2 business days for someone from the security team to respond to your disclosure request.

Please allow up to 4 weeks for the processing of payments for bounty rewards. Rewards are paid via bank transfer and require an invoice being sent to us detailing

- Your full name and email address
- The reward amount (agreed with Tribepad after reviewing report)
- The company you are requesting money from (Tribepad Ltd.)
- Reason for payment (bug bounty reward)
- The bank account to be paid, including
    - Bank name

    - Bank address
- Date and time

## 1.2 Terms and conditions

Any vulnerabilities that are discovered by participants are to be i) reported via the specified communication channel to Tribepad and ii) **must not** be reported directly to any of Tribepads clients.

All participants of the program:

**Must**

- Respect the sensitivity of any discovered vulnerabilities
- Respect the privacy of Tribepad
- Disclose vulnerabilities **only** to security@tribepad.com
- Retest any discovered vulnerabilities when prompted (for eligibility of reward)

**Must not**

- Report discovered vulnerabilities to Tribepad clients
- Attempt to access any accounts or private data that does not belong to you
- Attempt to modify or destroy any data of accounts that do not belong to you

Failure to adhere to any of the above will result in no bounty reward and possible legal action being taken, depending on the nature, severity and the sensitivity of the situation.

## 1.3 Report style

When reporting discovered vulnerabilities to us, please ensure that the following details are included

- Issue title
- Vulnerability type
- How does it impact the system and/or user(s)?
    - Impact level
    - Impact description
- What can be done to mitigate and/or remediate the issue?
    - Techniques to apply to code (where applicable)
    - Techniques to apply to infrastructure (where applicable)
    - Explain / expand where possible.
- Please provide a proof of concept

Failure to include relevant details will result in lack of reward.

## 1.4 System scope

The following URLs are in scope for the program. **Do not test** outside of these domains.

- https://testing.tribepad.uk
- https://tribepad.com
- https://manage.tribepad.com
- https://insights.tribepad.com

## 1.5 Vulnerability scope

Accepted vulnerabilities are listed below.

**NOTE**: Accepted vulnerabilities are only considered eligible when a proof of concept for the exploit is provided **AND** proves that the Confidentiality, Integrity or Availability of the data / information / asset is impacted negatively. If participants are unable to prove this, then the report will be ineligible for bounty rewards and won't be accepted.

- Information disclosure (only eligible if the information is **Confidential / Sensitive such as PII or account details AND originates from our systems, NOT compromised PCs of users**)
- Cross site scripting (XSS)
- SQL injection
- Open redirect
- Remote code execution (RCE)
- File upload vulnerabilities
- Server Side Request Forgery (SSRF)
- Privilege escalation and account takeover
- Insecure direct object reference (IDOR)
- Web cache poisoning
- Cross origin resource sharing (CORS)

## 1.6 Vulnerability exclusions

The following types of attacks and vulnerabilities are **excluded** from the scheme and will **NOT be accepted**. Please refrain from performing / raising the following:

- Missing security headers
- Host header vulnerabilities
- Missing Content Security Policy (CSP)
- Cross site request forgery (CSRF)
- Missing DNS and email records
- Blind vulnerabilities such as blind SSRF or blind SQLi

- Password policy rules and complexity
- Outdated libraries and components
- Social engineering and Phishing (and attacks requiring these)
- Brute force attacks
- Man in the middle (MITM) attacks
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Spamming
- Physical attempts against Tribepad premises and data centres
- Email address verification on account creation
- Session logout after password reset
- Lack of rate limiting

Rewards will be not be **eligible** under the following circumstances:

- Discovered vulnerabilities are already known by Tribepad (these will be classed as duplicates)
- Discovered vulnerabilities are disclosed to Tribepad clients
- Discovered vulnerabilities are against a product and/or feature that is either i) being decommissioned or ii) is currently unused

**Excluded** platform features include:

- Groups
- Communities
- Clusters
- Connections
- Messages

These areas of the platform **will not** be eligible for rewards.

## 1.7 Reward criteria and definitions

Please find our definitions of each severity / impact level below. This is what we will be accepting for the level rewards.

| **Severity / Impact** | **Amount (in GBP)** |
|---|---|
| Critical | £300 |
| High | £175 - £250 |
| Medium | £75 - £150 |
| Low | £25 - £50 |
| Accepted risk or informational | No reward. |

### 1.7.1 Critical

- Tribepad servers, databases or personal data records can be compromised via the web application which results in privilege escalation, data extraction, data damage or account takeover.
- Informational or enumeration counts here if the information is a database, server or administrator user password.

### 1.7.2 High

- The vulnerability exploit is possible on multiple accounts, resulting in privilege escalation, data damage, data leak or account takeover of other user accounts.
- User impact:
    - Affects multiple candidate accounts that do not belong to the participant.
    - Affects multiple recruiter accounts through privilege escalation.
    - Privilege escalation must originate from the candidate account.

### 1.7.3 Medium

- The vulnerability exploit is possible on multiple accounts, only resulting in data damage or defacement.
- User impact:
    - Affects multiple candidate accounts that do not belong to the participant.
    - Affects multiple recruiter accounts that do not belong to the participant.

### 1.7.4 Low

- The vulnerability exploit is possible on the account in use and does not lead to other accounts.
- User impact:
    - Affects a single candidate account that belongs to the participant.
    - Affects a single recruiter account that belongs to the participant.