

# Responsible Vulnerability Disclosure Program

Version: 1.0  
Publication Date: 20/01/2021  
Status: Current

<b>1.0 Vulnerability disclosure program</b>	<b>2</b>
1.1 Service level agreement	2
1.2 Terms and conditions	2
1.3 Report style	3
1.4 Disclosure scope	3
1.5 Exclusions	4
1.6 Reward criteria and definitions	4
1.6.1 Critical	5
1.6.2 High	5
1.6.3 Medium	5
1.6.4 Low	5

## 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](mailto: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.

### 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](mailto: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 (severity)
  - 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 Disclosure scope

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

- <https://windmill.tribepad.com/>

Accepted vulnerabilities include:

- Enumeration
- Stored XSS
- Reflected XSS
- SQLi
- CSRF
- RCE
- Token Vulnerability
- Unrestricted file upload
- SSRF
- Privilege escalation



## 1.5 Exclusions

The following types of attacks are **excluded** from the scheme. Please refrain from the following:

- Social engineering
- Denial of service
- Spamming
- Physical attempts against Tribepad and data centres

Rewards will be **ineligible** 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

## 1.6 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 <b>(unless the information is critical such as a password)</b>	No reward.



## 1.6.1 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.

## 1.6.2 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.

## 1.6.3 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.

## 1.6.4 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.

The table below shows the vulnerabilities and payouts that fit within these brackets.

Vulnerability Type	Payout			
	Low	Medium	High	Critical
Enumeration	£25	£75		
Stored XSS	£50	£100	£200	£300
Reflected XSS	£50	£100	£200	£300
SQLi	£50	£150	£250	£300
CSRF	£25	£75	£175	
RCE			£250	£300
Token Vulnerability	£25	£75	£175	£300
Unrestricted file upload	£50	£100	£200	£300
SSRF	£50	£150	£250	£300
Privilege escalation			£250	£300

