Responsible Disclosure Policy

We at Rupeek are committed to protecting our customer's privacy and ensuring that our customers have a safe and secure experience with us. If you discover a security vulnerability in our platform we appreciate your support in disclosing it to us in a responsible manner under the Rupeek Responsible Disclosure program (the "**Program**"). Before reporting the vulnerability, please be sure to review this policy ("**Policy**"). By participating in this Program, you agree to be bound by this Policy.

Responsible Disclosure

If you comply with the following while reporting a security vulnerability, we will not pursue any legal action or law enforcement activity against you.

- Report your finding by writing to us at disclosure@rupeek.com without making any information public. We will confirm a reply within 72 working hours of submission.
- Information about any vulnerability you've discovered must be kept confidential between Rupeek and you ("R**eporter"**) including the people involved in discovering the finding with the Reporter, until we have resolved the problem.
- You will make every effort to avoid privacy violations, disruption to production systems, degradation of user experience and destruction of data during security testing.
- You will not exploit a security issue you discover for any reason that affects reliability/integrity of our services or data. (This may include demonstrating any additional risk, such as compromise of sensitive company data or probing for additional issues.)
- You must perform research only within the scope.
- You shall not attempt to gain access to another user's account or data, perform DDoS or spam attacks. You shall also never attempt any non-technical attacks such as social engineering, phishing, or physical attacks against our infrastructure, users or employees.
- Only target your own accounts in the process of investigating any bugs/findings. Don't target, attempt to access, or otherwise disrupt the accounts of other users without the express permission of our team.
- In case you find a severe vulnerability that allows system access, you must not proceed further.
- It is Rupeek's decision to determine when and how bugs should be addressed and fixed.
- Disclosing bugs to a party other than Rupeek is forbidden, all bug reports are to remain at the reporter and Rupeek's discretion.
- Threatening of any kind will automatically disqualify you from participating in the program.
- Exploiting or misusing the vulnerability for your own or others' benefit will automatically disqualify the report.
- Bug disclosure communications with Rupeek's Security Team are to remain confidential. Researchers must destroy all artifacts created to document vulnerabilities (POC code, videos, screenshots) after the bug report is closed.
- Zero-day vulnerabilities or recently disclosed CVE will not be considered eligible until more than 90 days have passed since patch availability.

Scope

- https://www.rupeek.com
- Rupeek mobile app - Android, iOS and Windows

Reporting guidelines

Please include the following information when sending us the details:

- Operating System name and version.
- Browser name and version.
- Plugin names and versions installed in the browser.
- Steps necessary to reproduce the vulnerability including any specific settings required to be reproduced (If this contains more than a few steps, please create a video so we can attempt to perform the same steps).
- A copy of the HTML source code following your successful test.
- Probable impact of the issue.
- Scenarios leveraging this vulnerability
- Suggestions/Recommendation to fix the issue
- Provide details of the Reporter including Name etc. if not anonymous.
- Anything else that is deemed fit for understanding the finding/vulnerability.

Legal terms:

By participating in, you acknowledge that you have read and agree to Rupeek Terms of Service as well as the following:

- Your participation in the Program will not violate any law applicable to you, or disrupt or compromise any data that is not your own.
- You are solely responsible for any applicable taxes, withholding or otherwise, arising from or relating to your participation in the Program, including from any bounty payments.
- You will not under any circumstances disclose any vulnerability in social media, blogs etc. except with a written approval from Rupeek.
- Rupeek reserves the right to terminate or discontinue the Program at its discretion.

OUR RECOGNITION :

If you identify a valid security vulnerability in compliance with this Responsible Disclosure Policy, Rupeek shall

- Acknowledge receipt of your vulnerability report
- Work with you to understand and validate the issue
- Address the risk as deemed appropriate by Rupeek's team
- Work together to prevent cyber-crime.
- Rupeek will review the submission to determine if the finding is valid and has not been previously reported.
- Bug Bounty Program offers bounties for security software bugs and a digital certificate of recognition post validation of the bug

Publicly disclosing the submission details of any identified or alleged vulnerability without express written consent from Rupeek will deem the submission as noncompliant with this Responsible Disclosure Policy