Thank you for your interest in participating in Collibra's bug bounty program (the "**Program**"). The Program allows for the confidential disclosure of vulnerabilities to Collibra in our continuous efforts to enhance the security of our technology assets. A "**vulnerability**" under the Program is defined as a flaw in a computer system that weakens the overall security of the device/system, excluding issues identified as Out of Scope below. Subject to your compliance with the Program Rules outlined below, you may be eligible to receive a reward of between $10 and $500 per Vulnerability, depending on the severity of the Vulnerability, as determined by Collibra in its sole discretion ("**reward**"). Collibra evaluates the severity of reported vulnerabilities based on their impact and exploitability, based loosely on the prevailing Common Vulnerability Scoring System standard, however final determination as to the severity of a vulnerability and the associated reward is within Collibra's sole discretion. Collibra is committed to addressing responsibly disclosed Vulnerabilities in a timely manner and will endeavor to notify you of the remediation of any vulnerabilities you disclose.

Out of scope

The following issues are considered **"Out of scope"** from the Program and not deemed a Vulnerability under the Program:

- Clickjacking on pages with no sensitive actions
- Unauthenticated/logout/login CSRF
- Assets or resources prefixed with "console-"
- DNS removal of subdomains that do not point to an active service
- Attacks requiring MITM or physical access to a user's device
- Previously known vulnerable libraries without a working Proof of Concept
- Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Missing best practices in SSL/TLS configuration
- Third party service provider issues
- Any issues known to Collibra at the time of the reporting, or reported by a third party prior to your reporting the same to Collibra

For each report, please allow Collibra sufficient time to patch related paths. If you find the same bug on a different (unique) path, prior to the report being paid out, file it within the existing report to receive an additional 5% bonus (per path). Any reports filed separately while we are actively working to resolve the issue will be treated as a duplicate.

Program Rules

Eligibility for a reward under the program requires compliance with the following "**Program Rules**":

- Rules of disclosure:
  - Disclose the vulnerability confidentially, without disclosing to third parties, via security-vulnerability@collibra.com.
  - Provide detailed reports on the vulnerability with information sufficiently detailed for Collibra to reproduce the vulnerability on its own.
  - Multiple Vulnerabilities caused by one underlying issue are treated as a single Vulnerability.
- Prohibited activities:
  - Please use your own account for testing or research purposes. Do not attempt to gain access to another user's account or confidential information.
  - Social engineering of our users, employees, customers, partners, etc. (e.g. phishing, vishing, smishing) is prohibited.
  - Please do not engage in any activity that can potentially or actually cause harm to Collibra, our customers, or our employees.
  - Destruction of data, privacy violations, and the interruption or degradation of our services, such as Denial-of-Service, is prohibited.
  - Do not store, share, compromise, or destroy Collibra or customer data. If personal data is encountered, you should immediately halt your activity, purge related data from your system, and immediately contact Collibra.
  - Do not engage in any activity that violates (a) federal or state laws or regulations or (b) the laws or regulations of any country where (i) data, assets, or systems reside, (ii) data traffic is routed, or (iii) you are conducting research activity.