



Responsible Disclosure Policy

1. Overview

Data security is a top priority for dbt Labs, and dbt Labs believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in dbt Labs's service, it is of critical importance that you notify the Security Team. They will work with you to resolve the issue promptly.

2. Disclosure Policy

If you believe you've discovered a potential vulnerability, please let us know by emailing us at security@dbtlabs.com. We will acknowledge your email as soon as possible. In the worst case, we will acknowledge your report within one week.

Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within one week of disclosure. Non-critical issues will be prioritized according to severity.

Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the dbt Labs service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

3. Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of dbt Labs employees, contractors, or of dbt community spaces such as dbt Slack or Discourse
- Any attacks against dbt Labs' physical property or data centers
- Load testing dbt Cloud's production environment without written consent from the Security Team



- Signing up for multiple trials of dbt Cloud without written consent from the Security Team

Thank you for helping to keep dbt Labs and our users safe!

4. Bug Bounty Program

dbt Labs has contracted with HackerOne to provide both the platform to communicate with security researchers, as well as the pool of security researchers. We have very explicit rules of engagement that every researcher will have to agree to before they begin testing via HackerOne. Our security researchers are added to our Bug Bounty Program by invitation only. We have a limited number of licenses available, if you have a HackerOne account and are interested in participating, please contact security@dbtlabs.com.

5. Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available at <https://dbtlabs.com/disclosure>.

6. Contact

dbt Labs is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us security@dbtlabs.com

7. Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. dbt Labs management will determine how serious an employee's offense is and take the appropriate action.

8. Responsibility

It is the Security Team's responsibility to ensure that this policy is enforced.