Vendr 501 Boylston St. 10th Floor
Boston, MA 02116

Vendr Responsible Disclosure Policy

1. Purpose

Data security is a top priority for Vendr, and Vendr believes that working with skilled security researchers can identify weaknesses in any technology. If you believe you've found a security vulnerability in Vendr's service, please notify us; we will work with you to resolve the issue promptly. Thank you for helping to keep Vendr and our users safe.

2. Standards

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at security@vendr.com. We will acknowledge your email within five business days.
- 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 five business days of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Vendr 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 Vendr employees or contractors
- Any attacks against Vendr's physical property or data centers

4. Changes

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

5. Contact

Vendr is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@vendr.com.

6. Responsibility

It is the CTO's responsibility to see this policy is enforced.

Versioning

Date	Summary of Changes	Approval
4/28/20	Original	CTO
12/15/21	Formatting adjustments	Compliance Committee