Turvo, Inc.

Responsible Disclosure Policy

Effective Date: April 1, 2021

Program Overview

Data security is a top priority for Turvo, and Turvo believes that working with skilled security researchers can identify weaknesses in any technology. If you believe you've found a security vulnerability in our website, platform, or applications, please notify us; we will work with you to resolve the issue promptly.

Reporting a Potential Vulnerability

- Please promptly share details of the suspected vulnerability with the Turvo security team by emailing security@turvo.com.
- Provide the time, date, operating system, platform and browser used, and other details sufficient to enable us to reproduce the vulnerability by using a similar tool. This will help us gather appropriate information and expedite a response.
- Please do not disclose the issue to the public or to any third party until Turvo has had a reasonable opportunity to assess, confirm and resolve the vulnerability you reported.
- Turvo will attempt to review and respond to your report as soon as we can.

Activities That Are Not Permitted

- Please do not abuse any email addresses in the @turvo domain. In addition, do not abuse any 'Contact Us' forms, especially those that will initiate an email being sent.
- Please do not test physical office access (doors, tailgating, windows, etc.).
- Please do not engage in spamming, social engineering or phishing of Turvo employees.
- Please do not threaten or take actions to harm Turvo directors, officers, employees, customers, or members or engage in unprofessional conduct, such as aggressive language, extortion or harassment.
- Please do not perform any disruptive testing such as load or performance testing including Denial of Service attacks, or take other actions that interfere with the confidentiality, integrity, availability or operation of our sites, information, or applications. If you notice performance degradation on target systems, please stop use of automated tools.
- Please do not alter the content of Turvo's websites, applications, or social media accounts.
- Please do not alter privileges or login credentials.

Changes

We may revise these guidelines from time to time.

Contact

If you have any questions about this policy, please contact security@turvo.com.