# Orderful Security Vulnerability Disclosure Policy

## Overview

Orderful maintains robust measures to protect the security of its applications, systems, infrastructure, and customer data. We recognize the important role that independent security researchers play in keeping our technology ecosystem safe. This policy outlines how external parties can report security vulnerabilities to Orderful and what they can expect from us in return.

We are committed to working with security researchers to verify, reproduce, and respond to legitimate reported vulnerabilities. We will work in good faith to resolve any vulnerabilities reported to us and will ensure reporters are recognized for their efforts (with their permission). **Please note that we do not have a bug bounty program at this time.**

To maintain a high standard of security assurance, we engage an independent third party to conduct full-scope penetration testing and vulnerability assessments at least annually. These evaluations ensure that all Orderful services are developed and deployed in alignment with security best practices. These reports are available in our trust center, **trust.orderful.com**.

## Scope

This policy applies to any digital assets owned, operated, or maintained by Orderful, including but not limited to:

- All Orderful applications and APIs
- All marketing materials published by Orderful
- Open source projects maintained by Orderful
- Infrastructure and systems that directly support Orderful services

## How to Report a Security Vulnerability

### Reporting Channel

Please report all security vulnerabilities via email to: **security@orderful.com**

### Information to Include

When reporting a vulnerability, please provide as much of the following information as possible:

- **Type of vulnerability** (e.g., SQL injection, cross-site scripting, authentication bypass)
- **The affected product/service**

- **Step-by-step instructions** to reproduce the vulnerability
- **Proof-of-concept code** or screenshots demonstrating the issue
- **Impact assessment**, your understanding of the potential impact
- **Your contact information** for follow-up questions
- **Whether you wish to be acknowledged** for your discovery

## Our Commitment to Reporters

When you report a security vulnerability to Orderful, we commit to:

#### Response Timeline

- **Initial acknowledgment**: Within 5 business days of receiving your report
- **Initial assessment**: Within 15 business days, we will provide an initial assessment of your report and, if valid, an expected timeline for resolution
- **Resolution notification**: We will notify you when the vulnerability has been fixed

#### What We Promise

- We will not pursue legal action against researchers who follow the “Guidelines for Security Researchers” section below
- We will work to understand and resolve the issue within a reasonable time frame
- We will recognize your contribution publicly (with your permission) once the issue is resolved

## Guidelines for Security Researchers

To ensure a productive relationship between Orderful and the security research community, we ask the following:

#### Please Do

- Allow us reasonable time to respond to your report and provide a fix
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service
- Only interact with test accounts you own or with explicit permission from the account holder
- Provide sufficient information to reproduce and validate the vulnerability
- Delete any data retrieved during security research promptly after reporting

#### Please Don't

- Access, modify, or delete other users' data without explicit permission
- Perform actions that could harm the reliability or integrity of our services (e.g., denial of service attacks).

- Exploit vulnerabilities beyond the minimum necessary to verify the issue
- Use automated scanners that generate excessive traffic
- Share vulnerability details publicly before we've had adequate time to address the issue
- Demand compensation or rewards as a condition for responsible disclosure.  Again, we do not have a Bug Bounty program at this time.

### Out of Scope

The following types of reports are generally considered to be out of scope for this kind of external reporting:

- Vulnerabilities in third-party services not under our control
- Social engineering attacks
- Physical security issues
- Reports from automated scans without verification
- Issues that require significant user interaction or unlikely user behavior
- Disclosure of known public information
- Spam, phishing, or malware issues unrelated to our infrastructure
- Vulnerabilities in outdated versions of browsers or platforms
- Best practice concerns without demonstrable security impact

### Recognition

With your permission, we will acknowledge security researchers who help us improve our security posture on our Security Acknowledgments page.

### Safe Harbor

Orderful considers security research activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act, the DMCA, and other applicable computer crime laws. We will not initiate or support legal action against you for security research activities conducted in accordance with this policy.

If legal action is initiated by a third party against you for activities conducted in accordance with this policy, we will make it known that your actions were conducted in compliance with this policy.

### Contact Information

- **Security Reports, Questions, Inquiries**: security@orderful.com

### Policy Updates

This policy may be updated from time to time. The latest version will always be available at:

**https://orderful.com/vulnerabilty-disclosure**

**Written by**: Jared Daley

**Last Updated**: August 12, 2025

**Version**: 1.0