Point Blue
Conservation
Science

3820 Cypress Drive #11, Petaluma, CA 94954
T 707.781.2555 | F 707.765.1685

Point Blue Conservation Science Vulnerability Disclosure Policy

Version 1.0

At Point Blue, protecting the security of our systems and data is paramount. As part of our commitment to safeguarding both our organization and those who rely on our services, we encourage the responsible reporting of any security vulnerabilities you may find. This policy is designed for security researchers, ethical hackers, and anyone who discovers a potential security vulnerability within our systems or applications.

If you believe you've identified a vulnerability, please read this policy carefully before testing or reporting. Your adherence to these guidelines will help us address issues quickly, while ensuring a safe, legal, and collaborative process.

Purpose of This Policy

This vulnerability disclosure policy outlines how you can report potential security issues to us. By providing a clear process for vulnerability disclosure, we aim to foster responsible security research that enhances the integrity of our systems and protects our data. In line with best practices, we commit to working with security researchers to verify and address any vulnerabilities reported.

Reporting a Potential Vulnerability

If you identify a potential vulnerability in Point Blue's website, applications, or other online services, please contact our security team as soon as possible. To report an issue:

- **Email us at**: InfoSec@pointblue.org
- **Use Encrypted Communication**: For security, we ask that you send your report using encrypted communication methods. Upon receiving your email, you should receive an automatic acknowledgment. If you don't receive a response, please verify the email address and try again.
- **Provide Details**: To help us investigate the issue efficiently, include a detailed description of the suspected vulnerability in your report. This will allow our security team to validate and reproduce the problem as needed.

Our security team will review and investigate your report. For the protection of all users, we generally do not disclose or confirm security issues until a full investigation is complete and any necessary fixes are available.

Responsible Disclosure Guidelines

We welcome and encourage responsible security research, but we ask that you refrain from any actions that might disrupt our services or harm our users. Please avoid the following:

- **Disruptive Testing**: Avoid brute force attacks, denial-of-service attempts, spam, or other actions that could impair Point Blue's services.
- **Unauthorized Data Access**: Do not attempt to access, modify, or destroy data that does not belong to you.
- **Physical or Electronic Attacks**: Refrain from any physical or electronic attacks against Point Blue's personnel, property, or partner data centers.
- **Social Engineering**: Do not attempt to deceive or manipulate any Point Blue employees, contractors, or service desks.
- **Testing Outside of Authorized Accounts**: Conduct testing only on test accounts that you have created.
- **Violation of Laws or Agreements**: All testing must comply with applicable laws and agreements.

If you follow these guidelines, Point Blue pledges not to pursue legal action for vulnerability testing that aligns with this policy.

Recognition

We value and appreciate the efforts of researchers who work responsibly to help us improve our security. Thank you for your commitment to making Point Blue safer for everyone.