Vulnerability Disclosure Policy

At Dimensions Technologies, we take the security of our systems, services, and customer data seriously. We welcome reports from security researchers, customers, and members of the public who believe they have discovered a security vulnerability in our products or services.

This policy outlines how to report vulnerabilities and what you can expect from us in return.

Reporting a Vulnerability

If you believe you have identified a security vulnerability in a Dimensions Technologies system, product, or service, please report it by email to:

security@dimensions.team

Please include as much of the following information as possible:

- A description of the vulnerability
- The affected system, application, or URL
- Steps required to reproduce the issue
- Any proof-of-concept code or screenshots
- The potential impact of the vulnerability
- Your contact details for follow-up questions

We encourage encrypted submissions where appropriate. Our PGP public key is available upon request.

Our Commitment

When you submit a vulnerability report in good faith, we will:

- Acknowledge receipt of your report within 3 business days
- Review and assess the reported issue
- Keep you informed of the progress of our investigation where appropriate
- Work to remediate confirmed vulnerabilities in a timely manner
- Credit you for your discovery, if desired and appropriate

Scope

This policy applies to systems and services owned and operated by Dimensions Technologies, including:

- Public-facing websites
- Customer portals
- Hosted services and APIs
- Mobile and desktop applications maintained by Dimensions Technologies

Out of Scope

The following activities are not authorised under this policy:

- Denial-of-service (DoS or DDoS) testing
- Physical attacks against company facilities
- Social engineering of employees, contractors, or customers
- Spam, phishing, or unsolicited communications
- Testing against third-party services not owned or controlled by Dimensions Technologies
- Accessing, modifying, deleting, or downloading customer data beyond what is necessary to demonstrate a vulnerability

Rules of Engagement

This policy applies to systems and services owned and operated by Dimensions Technologies, including:

- Act in good faith
- Avoid privacy violations, service disruption, and data destruction
- Use only the minimum amount of testing necessary to confirm the existence of a vulnerability
- Immediately stop testing and notify us if you encounter customer data
- Do not publicly disclose details of the vulnerability until we have had a reasonable opportunity to investigate and remediate the issue

Safe Harbour

Dimensions Technologies considers security research conducted in accordance with this policy to be authorised.

We will not pursue legal action against individuals who:

- Make a good-faith effort to comply with this policy
- Avoid causing harm to customers, users, or our services
- Report vulnerabilities promptly and responsibly
- Do not exploit vulnerabilities beyond what is necessary to demonstrate their existence

If legal action is initiated by a third party against a researcher who has complied with this policy, we will make it known that the research activity was conducted in accordance with our Vulnerability Disclosure Policy.

Disclosure and Remediation

Our goal is to investigate all legitimate vulnerability reports and address confirmed issues as quickly as possible. Remediation timelines will vary depending on the severity, complexity, and potential impact of the vulnerability.

We may coordinate public disclosure with the reporting party once a vulnerability has been resolved.

Questions

If you have questions regarding this policy or wish to report a vulnerability, please contact:

security@dimensions.team