

Responsible Disclosure Policy

At Degreed, the security and integrity of our platform are of utmost importance. We are committed to safeguarding the data entrusted to us by our customers, employees, and partners, ensuring it remains protected and secure at all times.

A key part of our security program is responsible disclosure. We encourage and greatly appreciate security researchers to contact us to report any potential vulnerabilities found in our products or other digital assets.

If you have identified a potential security vulnerability, please share it with us by following the guidelines below. We'd appreciate your cooperation by adhering to the following principles:

Please do not publicly disclose the vulnerability before we've had a reasonable amount of time to mitigate the vulnerability.

Maintain an open line of communication so we can work together to resolve the issue, and share the learnings so others don't make the same mistakes.

Refrain from actions that would harm service to our customers by creating a degradation or disruption of service, including loss or manipulation of data.

Do not store, share, manipulate or destroy Degreed or customer data. If you should gain access to Personally Identifiable Information (PII) please halt your activities, purge the data from your systems, and contact us immediately.

Our Commitments to You

By responsibly submitting your findings to Degreed Security in accordance with these guidelines Degreed agrees not to pursue legal action against you. Degreed reserves all legal rights in the event of noncompliance with these guidelines.

Once a vulnerability report is submitted, Degreed Security commits to provide prompt acknowledgement of the receipt of the report (within three business days of submission) and will keep you reasonably informed of the status of any validated vulnerability that you report through this program.

Submission Format & Instructions

When submitting a report of a potential vulnerability, please include a detailed summary of the vulnerability, including the target, steps, tools, and artifacts used during discovery (screen captures welcome).

Please email the report to Degreed Security at security@degreed.com.

Please note that Degreed does not operate a bug bounty program and we do not offer reward nor compensation in exchange for the identification of potential issues.