Vulnerability Disclosure Policy

1 Introduction

We understand the importance of security researchers in assisting us in maintaining a high level of security and privacy. Coordination of vulnerability research, mitigation, and disclosure is part of this policy. This policy defines good faith in the context of detecting and reporting vulnerabilities.

2 Scope

This policy applies to all individuals who engage in security testing and vulnerability discovery against zeiss.com and its subdomains as well as non medical ZEISS products.
By participating in vulnerability discovery, all individuals agree to abide by the terms and conditions outlined in this policy.

3 Guidelines

A reproducible research report is crucial to confirming and addressing an issue as quickly as possible.

A comprehensive report includes:

- Clear explanation of the issue(s) and the observed behavior, as well as the expected behavior.
- Detailed information about the affected product (e.g serial number and description) or website (e.g url).
- Detailed list of the steps needed to reproduce the problem.
- Reliable evidence for the issue you are describing.
- Specifics about any related issues.

Vulnerability reports with greater specifics are well appreciated. We look forward for your submissions including below listed points

- The report consists of the necessary details to allow us to duplicate the issue.
- No Results from automated tools or scans.
- Vulnerability reports shall include communication details. (eg. Valid contact information.

4 Responsible Disclosure

Researchers are expected to adhere to responsible disclosure principles. This means that if a security vulnerability or weakness is discovered, it should always be reported immediately to ZEISS via email to **vulnerability-disclosure@zeiss.com**.
Vulnerability reports are usually considered confidential and should be sent encrypted. Please use the provided PGP key for establishing an encrypted communication with us. The public disclosure of the vulnerability is allowed only in coordination with ZEISS.

5 Unauthorised Activities

Researchers must strictly adhere to the following guidelines and refrain from engaging in any unauthorized activities:

5.1 Modifying or deleting data without explicit permission.

5.2 Conducting any activity that may result in the degradation or disruption of services.

5.3 Compromising the privacy or confidentiality of user data.

5.4 Executing any form of Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.

5.5 Sharing or disclosing any sensitive information obtained during the research process, except with explicit consent from ZEISS.

6 Legal Compliance

Researchers must ensure that all activities conducted during their security research comply with applicable local, regional, and international laws, regulations, and policies. ZEISS will not

provide any legal assistance or protection to researchers involved in illegal or unauthorized activities.

7 Non-Disclosure and Confidentiality

Researchers must respect the confidentiality and privacy of the information and data obtained during their security research. Researchers must not disclose, share, or utilize any confidential or proprietary information acquired during their engagement without explicit permission from ZEISS.

8 Safe Harbour

ZEISS commits to a safe harbor policy for researchers who comply with this policy. As long as researchers act in good faith and adhere to the guidelines specified in this policy, ZEISS will not pursue legal action against them related to their security research activities.

9 Acknowledgment

By participating in ZEISS vulnerability discovery and disclosure program, researchers acknowledge that they have read, understood, and agree to comply with the terms and conditions outlined in this Security Policy.

10 ZEISS Commitment

By following the ZEISS Security Disclosure Policy, ZEISS will use reasonable efforts to:

- Respond quickly and acknowledge receipt of the vulnerability report
- Notify the reporting party when the vulnerability has been fixed

Our standard response time to acknowledge receipt of vulnerability reports is 5 working days (this means that it excludes weekends and public holidays from Germany). Status updates of reported vulnerabilities are given when relevant information becomes available.

11 Contact Information

For any questions, concerns, or reports related to security vulnerabilities or this Security Policy, please write to **vulnerability-disclosure@zeiss.com**.