Vulnerability Disclosure Process

At Elisian Ltd, we develop technologies to advance and optimize the efficiencies of our customers. To achieve this, we uphold core values that define our responsibility to those we serve. Among them: an unwavering commitment to the safety and security of patients and safety personnel. Therefore, we believe in continuously improving to address the ever-evolving privacy and cybersecurity landscape.

In response to potential threats to cybersecurity, Elisian Ltd has formed a product security team to assess vulnerabilities and determine responses within a vulnerability disclosure process. These efforts allow the company to continually learn from vulnerability test information submitted to us by customers and security researchers.

For the latest product detail information, please visit https://www.elisian.co.uk.

Scope

This process applies to the reporting of potential cybersecurity vulnerabilities in Elisian Ltd products only. Elisian Ltd marketing websites, e-commerce sites, and all other non-product systems are out of scope. Please do not engage in unauthorized testing of out of scope assets.

For customer support help requests, technical documents and regulatory contacts and notifications, please contact support.

Contact information and submission process

Potential security vulnerabilities or privacy issues with a Elisian Ltd product should be reported to: dpo@elisian.co..uk

We ask that you please refrain from including sensitive information (e.g., sample information, PHI, PII, etc.) as a part of any submissions to Elisian Ltd. Please provide the following information in your submission:

- Your contact information (e.g., name, address, phone number, and email)
- Date and method of discovery
- Description of potential vulnerability
  - Product name
  - Customer
  - Configuration details
- Steps to reproduce

- Tools and methods
- Exploitation code
- Privileges required

- Results or impact

What happens next

Upon receipt of a potential product vulnerability submission, Elisian Ltd will:

- Acknowledge receipt of the submission within five (5) business days
- Work with specialized product teams to evaluate and validate reported findings
- Contact the submitter to request additional information, if needed
- Take appropriate action

Elisian Product Security Team

2nd April 2025

Disclaimer

Elisian Ltd considers it a top priority to protect the health and safety, as well as the personal information, of our customers' patients and safety personnel.

When conducting your security research, please avoid actions that could cause harm to patients or products. Note that vulnerability testing could negatively impact a product. As such, testing should not be conducted on active products, and products subjected to security testing should not subsequently be used in a clinical setting. If there is any doubt, please contact a Elisian Ltd representative.

Elisian Ltd reserves the right to modify its coordinated vulnerability disclosure process at any time, without notice, and to make exceptions to it on a case-by-case basis. No particular level of response is guaranteed. However, if a vulnerability is verified, we will attribute recognition to the researcher reporting it, if requested.

CAUTION: Do not include sensitive information (e.g., sample information, PHI, PII, etc.) in any documents submitted to Elisian Ltd. Comply with all laws and regulations in the course of your testing activities.

By contacting Elisian Ltd, you agree that the information you provide will be governed by our site's Privacy Policy and Online Terms of Use.

Note: When sharing any information with Elisian Ltd, you agree that the information you submit will be considered non-proprietary and non-confidential and that Elisian Ltd is allowed to use such information in any manner, in whole or in part, without any restriction.