# Vulnerability Disclosure Policy

## 1. Purpose

The purpose of this Vulnerability Disclosure Policy is to provide a clear and secure process for reporting potential security vulnerabilities in our products. We value the contributions of security researchers, customers, and partners in helping us maintain the safety, integrity, and availability of our products.

## 2. Scope

This policy applies to all software-enabled in vitro diagnostic (IVD) products, unless explicitly stated otherwise.

## 3. Reporting a Vulnerability

If you believe you have identified a security vulnerability, please report it to us via:
https://app.whistle.law/whistle/ - /5a474110-2abf-4d2d-8b37-92c1c9050789

Please do not include any sensitive information (e.g. patient data) in the documents provided to us.

Please include, where possible:

- Affected device: manufacturer, model, hardware version, firmware/software version
- A description of the vulnerability: What exactly did you observe, and what security implications do you suspect?
- Steps to reproduce the issue: A step-by-step description that is as detailed as possible, including prerequisites, required tools, and network location.
- Evidence: screenshots, logs, packet captures, sample requests, or other supporting documents. Please anonymize any personal or third-party data.
- Potential impact: What data, functions, or systems might be affected? Is physical access, local network access, or internet access required?
- Test environment: Did you test exclusively on your own or authorized devices? Was any third-party data viewed, modified, or transferred?
- Disclosure status: Has the vulnerability already been publicly disclosed or reported to other parties? Is a public disclosure planned?
- Necessary contact information (contact names, organization name, tracking numbers, email addresses, phone numbers) so that we can get in touch with you

## 4. Our Commitment

We commit to:

- Acknowledge receipt of your report within **5 business days** (prerequisite: contact information is provided)
- Assess the vulnerability in a timely manner
- Keep you informed about the status of your report, where appropriate (prerequisite: contact information is provided)
- Treat your Report confidentially
- Not pursue legal action against researchers acting in good faith and in accordance with this policy

## 5. Expectations for Responsible Disclosure

We ask that you:

- Act in good faith and avoid privacy violations, data destruction, or service disruption.
- Do not exploit the vulnerability beyond what is necessary to demonstrate it.
- Do not publicly disclose the vulnerability before we have had a reasonable opportunity to investigate and address it.
- Provide us reasonable time to remediate the issue before disclosure.

## 6. Evaluation and Handling

Reported vulnerabilities are:

- Assessed for severity, exploitability, and potential impact on patient safety, data integrity, and system availability.
- Integrated into our cybersecurity and risk management processes in accordance with applicable standards.

Vulnerabilities with potential impact on product safety are evaluated within the framework of risk management according to **ISO 14971**.

### 7. Remediation

Where necessary, we will:

- Develop and implement appropriate corrective actions (e.g. patches, mitigations)
- Validate the effectiveness of implemented measures
- Communicate relevant information to affected customers

### 8. Disclosure

Public disclosure (e.g. field safety notifications, security advisories or CVE publication) will be coordinated, where possible, with the reporting party and after appropriate remediation actions have been taken.

### 9. Integration into Post-Market Activities

All reported vulnerabilities are considered as input to our post-market surveillance and cybersecurity risk management processes.

### 10. Legal

This policy does not grant permission to access or modify data beyond what is necessary for responsible vulnerability research. Activities must comply with applicable laws and regulations.

### 11. Contact

For any questions regarding this policy, please contact:
info@analyticon-diagnostics.com

Signed on behalf of **Analyticon Biotechnologies GmbH**
Am Muehlenberg 10
35104 Lichtenfels, Germany


Dr. Stephan Busche
Managing Director
Place: Lichtenfels, Germany
Date: 10.08.2026