VARIOLYTICS
Making the invisible visible.

Coordinated Vulnerability Disclosure (CVD) Policy

Policy for the coordinated reporting and disclosure of security vulnerabilities

Company	Variolytics GmbH
Version	1.0
Last Updated	August 2026
Status	Released

1. Purpose of this Policy

The security of our products and systems is a high priority for Variolytics GmbH. Despite careful development, testing and ongoing security measures, vulnerabilities cannot be completely ruled out.

We therefore welcome reports from customers, security researchers and other third parties regarding potential security vulnerabilities in our products. This Coordinated Vulnerability Disclosure Policy explains how potential vulnerabilities can be reported to us and how we handle such reports.

Our objective is to investigate and remediate security vulnerabilities responsibly, confidentially and in a coordinated manner, while reducing risks to users, customers and systems as far as possible.

2. Scope

This policy applies to products with digital elements provided by Variolytics GmbH and the associated software, firmware and product-related digital components.

In Scope

- EmiCo lite (connected measurement device)
- EmiCo Insight (data-processing platform, cloud, on-premises IPC, or customer VM)
- firmware and embedded software of the products listed above
- associated software components
- associated cloud services, where they form part of the product functionality
- associated web applications and APIs
- product-related interfaces and update mechanisms provided by Variolytics
- third-party and open-source components insofar as they form part of our products.

Out of Scope

Unless expressly agreed otherwise, the following systems or activities are outside the scope of this policy:

- third-party systems or services that are not operated or controlled by Variolytics
- social engineering attacks against employees or contractors
- physical attacks against buildings, employees, devices or infrastructure

- denial-of-service or distributed denial-of-service testing
- spam, automated mass messaging or unnecessarily high automated request rates
- testing that may cause avoidable impairment of the availability, integrity or functionality of our products, systems or services.

If you are unsure whether a product, system or testing method is in scope, please contact us before carrying out further testing.

3. Reporting a Vulnerability

If you discover a potential vulnerability, please submit your report using the following contact details:

Security email	[security@variolytics.com]
Suggested subject	Security Vulnerability Report – [Product name]

To enable us to analyse your report efficiently, please include as much of the following information as possible:

- affected product or component
- model, firmware or software version
- description of the vulnerability and the observed impact
- steps required to reproduce the issue
- where applicable, a proof of concept, logs, screenshots or other technical evidence
- tools and testing methods used, where relevant to reproduction
- date or time of discovery
- information on whether the vulnerability is already known to third parties
- any intended publication timeline
- contact details for follow-up questions.

Please do not submit personal data, confidential information or other protected information that is not necessary for analysing the vulnerability.

4. How We Handle Your Report

After receiving a report, we review the information provided and assess the potential vulnerability. Our process generally includes the following steps:

1. Acknowledgement – We aim to acknowledge receipt of your report within 3 business days.
2. Initial assessment – We review whether the issue can be understood, which products are affected and what the potential security impact may be.
3. Technical analysis – Where necessary, we investigate and reproduce the reported vulnerability.
4. Risk assessment and prioritisation – Confirmed vulnerabilities are prioritised according to their risk and potential impact.
5. Remediation or mitigation – We develop appropriate corrective or risk-reduction measures.
6. Security update – Where required and technically feasible, we provide a security update or other suitable measures.
7. Coordinated disclosure – Where possible, the publication of information about the vulnerability is coordinated with the reporting party.

We aim to keep reporting parties informed about material progress. The time required to resolve a vulnerability depends in particular on its complexity and risk, the affected components and any necessary coordination with third parties.

5. Coordinated Disclosure

Please do not publish or share detailed information about an unresolved vulnerability without prior coordination with us.

In particular, we ask that you allow Variolytics sufficient time to analyse the vulnerability, develop and test an appropriate remediation, provide security updates and inform affected users where necessary.

Variolytics will in turn seek to address confirmed vulnerabilities without undue delay. Once an appropriate corrective measure is available, Variolytics and the reporting party may coordinate an appropriate timing and scope for publication.

In justified cases, publication may be delayed where premature disclosure would increase the security risk to users or systems.

6. Responsible Security Research

We ask security researchers to act in good faith, proportionately and responsibly. Please:

- perform only the testing necessary to identify and verify a vulnerability;
- avoid impairing the availability or functionality of our products and systems;
- do not access data belonging to other users and do not alter or delete data;
- do not copy data unless this is strictly necessary to demonstrate the vulnerability;
- stop testing if you inadvertently gain access to personal, confidential or otherwise protected information;
- do not conduct social engineering attacks;
- do not install malware or establish persistent access;
- do not exploit a discovered vulnerability for your own or another party's benefit;
- do not disclose information about a vulnerability to third parties before coordinated disclosure has taken place.

If you inadvertently access sensitive information during your research, stop accessing it and notify us immediately.

7. Treatment of Security Researchers

Where security research is conducted in good faith, within the scope of this policy and without malicious intent, Variolytics does not intend – to the extent legally permissible – to initiate legal action solely as a result of such security research.

This applies only where, in particular:

- the research is proportionate;
- no unnecessary damage or operational disruption is caused;
- data is not misused;
- no extortion or payment demand is linked to withholding publication of a vulnerability;

- the vulnerability is reported and disclosed in accordance with this policy.

> This statement does not constitute a general authorisation to violate applicable law, contractual obligations or third-party rights.

8. Security Updates and Information

Confirmed vulnerabilities are handled according to their risk. Where required, we provide security updates or other appropriate measures to remediate or reduce the risk.

Published security information may include, in particular:

- affected product and affected versions
- description and security impact of the vulnerability
- severity or prioritisation
- fixed version and available security updates
- required actions or recommendations for users.

Security information is published at: https://variolytics.com/security

9. Vulnerabilities in Third-Party Components

Our products may contain software, hardware or open-source components supplied by third parties. Where a reported vulnerability affects such a component, we may share information about the vulnerability with the relevant manufacturer, provider or maintainer where this is necessary for analysis and remediation and is legally permissible.

We seek to ensure that such information is shared in a coordinated and responsible manner.

10. Regulatory Reporting Obligations

Certain vulnerabilities or security incidents may be subject to statutory reporting obligations. Variolytics therefore reserves the right to share information about reported vulnerabilities with competent authorities, Computer Security Incident Response Teams (CSIRTs) or other bodies designated under applicable law, to the extent required by law.

This applies in particular to reporting obligations under Regulation (EU) 2024/2847 (Cyber Resilience Act).

11. Compensation

Variolytics does not currently operate a bug bounty programme. Reporting a vulnerability therefore does not generally give rise to any entitlement to financial compensation.

12. Contact

Company	Variolytics GmbH
Postal address	Ruppmannstraße 28, 70565 Stuttgart
Security contact	security@variolytics.com
Website	https://www.variolytics.com
CVD Policy	https://variolytics.com/security
Security advisories	https://variolytics.com/security

This policy may be updated from time to time. The version published on our website is the applicable version.