COORDINATED VULNERABILITY DISCLOSURE POLICY

Introduction

The security of our systems and the protection of our users' data are our highest priorities. To continuously improve the quality and security of our products, we encourage and welcome security-related feedback.

This Coordinated Vulnerability Disclosure (CVD) Policy outlines how you can report potential security vulnerabilities or data protection incidents to us responsibly, and what you can expect from us during the process.

Scope

This policy applies to all products, web applications, and IT systems of the Erbe Group.
Important: Only analyse devices with the explicit consent of their owner and always comply with applicable laws and regulations.
The following vulnerabilities are out of scope for this policy:

- Social engineering attacks (e.g. phishing)
- Availability attacks (e.g. DDoS)
- Attacks on third-party providers or partner services outside our control

If you are unsure whether a system is in scope, please contact us.

Reporting

To report a vulnerability, please contact us at: **security@erbegroup.com**

For an efficient review, please include the following information:

- **Description of the vulnerability**: A clear explanation of the issue
- **Affected product or component**: Include version numbers, URLs, IPs, or other relevant identifiers
- **Steps to reproduce**: Detailed steps or a proof of concept (PoC) to demonstrate the issue
- **Your contact information:** In case we need to follow up for additional details

Our commitments

- We will **acknowledge receipt** of your report promptly
- We will **keep you informed** throughout the process
- We will **notify** you once the vulnerability is resolved

Our expectations

If you report a vulnerability to us, we will not take legal action against you if the following conditions are met:

- Do not intentionally harm Erbe, our customers, their patients or third parties
- Respect the privacy and security of our customers and patients
- Report the vulnerability promptly upon discovery
- Do not publicly disclose the vulnerability until it has been resolved
- Refrain from violating any applicable laws

Thank you for your cooperation. Your responsible disclosures help us to identify and mitigate risks at an early stage.