BOWE GROUP

BOWE.COM

COORDINATED VULNERABILITY DISCLOSURE POLICY

BOWE GROUP

Version: 1.2

Effective as of: September 11, 2026

Classification: Public – for publication on bowe.com

BOWE GROUP
a brand of
BÖWE SYSTEC GmbH

TABLE OF CONTENTS

1. PURPOSE

The security of our products, services, and customers is a top priority for the BOWE GROUP. Despite careful development, quality assurance, and technical and organizational security measures, the occurrence of vulnerabilities cannot be completely ruled out.

This Coordinated Vulnerability Disclosure Policy (hereinafter "CVD Policy" or "Policy") describes how external security researchers, customers, and other parties can report potential security vulnerabilities in the BOWE GROUP's products, applications, and services, and how the BOWE GROUP handles such reports.

The purpose of this policy is to ensure the responsible, coordinated, and transparent handling of reported vulnerabilities in order to minimize risks to customers, systems, and the general public.

2. SCOPE

2.1 SCOPE

This policy applies to all products with digital elements that are manufactured by the BOWE GROUP, placed on the market in the EU, or operated within the EU.

2.2 EXCLUSIONS

- Systems, installations, or other devices that are not owned by the parties involved in this policy.

If vulnerabilities are discovered or suspected in systems not covered by this policy, please report them directly to the respective manufacturer, operator, or the competent authority.

3. REPORTING A SECURITY VULNERABILITY

Security vulnerabilities can be reported as follows:

Email: product-security@bowe.com

To ensure prompt processing, the report must include the following information:

- Affected product or system
- Affected customer (name, order number), if applicable
- Product version
- Description of the vulnerability
- Indication of whether active exploitation of the vulnerability is known
- Steps to reproduce

- Proof of concept, if available
- Contact Information for Inquiries

Please provide only the information necessary for assessing the vulnerability and refrain from submitting unnecessary personal or confidential third-party data.

The report may be submitted in German or English.

4. OUR COMMITMENTS

If you cooperate with us in accordance with this policy, you can expect us to:

- confirm receipt of your report within five business days and work with you to investigate and validate the reported vulnerability.
- keep you informed, to the extent possible and appropriate, of the progress of our investigation.
- promptly address identified vulnerabilities, taking into account operational and technical constraints, or implement appropriate risk-mitigation measures.
- grant the safe harbor protection described in Chapters 5 and 6 of this policy for security research conducted in accordance with those chapters.

5. EXPECTED CONDUCT OF SECURITY RESEARCHERS

We welcome good-faith security research and ask that the following rules be observed. Full compliance with these rules is a prerequisite for the safe harbor protection described in Chapter 6.

5.1 PERMITTED ACTIVITIES

- Identification and documentation of security vulnerabilities
- Conducting the minimum necessary tests for verification
- Reporting the vulnerability exclusively to the BOWE GROUP via the reporting channel specified in Chapter 3
- Treating findings as confidential
- Security investigations in one’s own test environments or in expressly authorized environments

5.2 PROHIBITED ACTIVITIES

- Accessing third-party data
- Modification or deletion of data
- Interruption of services
- Denial-of-service attacks

- Social engineering targeting employees or customers
- Installation of Malware
- Physical tampering with customer equipment
- Testing on customers' production systems without their express consent
- Tests on running machines
- Manipulation of PLC, CNC, robot, or machine control systems
- Changes to process parameters
- Bypassing safety or protective functions
- Activities that may affect occupational safety, plant safety, or product quality
- Load or stress tests on production OT systems

5.3 PROCEDURE IN THE EVENT OF UNINTENTIONAL DATA ACCESS

If sensitive or personal data is unintentionally accessed during testing activities, all activities must be stopped immediately. The incident must be documented as part of the reporting process; furthermore, the affected data must not be viewed, stored, further processed, or disclosed.

6. SAFE HARBOR

We do not intend to take legal action against security researchers who act in good faith and in accordance with this policy.

6.1 PREREQUISITE

The safe harbor protection described in this chapter applies exclusively if and to the extent that the reporting person fully and consistently complies with all conditions set forth in Chapter 5—in particular, that they:

- engages exclusively in the activities designated as permitted in Section 5.1,
- does not engage in any of the activities designated as prohibited in Chapter 5.2,
- acts immediately in the event of unintentional access to sensitive or personal data as described in Chapter 5.3, and
- reports the vulnerability exclusively through the reporting channel specified in Chapter 3.

6.2 SCOPE OF THE COMMITMENT

Provided that the requirements set forth in Section 6.1 are met, we consider the security research conducted as part of the report to be an activity authorized by the BOWE GROUP. We will not take any civil or criminal action against the reporting individual in connection with the discovery, investigation, and reporting of the vulnerability, and we will do everything in our power to ensure that third parties also refrain from doing so, provided that

the relevant activities were carried out on behalf of and at the request of the reporting individual in accordance with this policy.

6.3 LIMITS OF THE COMMITMENT

This commitment:

- applies exclusively to the specific vulnerability reported and the activities necessary for its verification;
- does not establish any separate claim against third parties (e.g., affected customers) and does not affect their own rights;
- does not apply to actions that violate applicable law independently of this policy;
- may be amended by the BOWE GROUP at any time for future reports; reports already submitted in compliance with the rules remain unaffected by any subsequent changes.

7. ASSESSMENT AND PRIORITIZATION

We strive to assess and respond to incoming reports in a timely manner.

Each reported vulnerability is evaluated in particular with regard to the following criteria:

- Exploitability
- Impact on confidentiality
- Impact on integrity
- Impact on availability
- Impact on functional safety

8. COORDINATED DISCLOSURE

We prefer coordinated vulnerability disclosure. The standard procedure is as follows:

1. Receipt of the report
2. Analysis and risk assessment
3. Development of a fix or mitigation
4. Provision of an update
5. Notification of affected customers
6. Release of a security advisory

We ask reporters to refrain from making the issue public until a fix has been provided or another course of action has been mutually agreed upon.

In cases required by law (particularly in the event of actively exploited vulnerabilities or serious security incidents), the BOWE GROUP may be subject to additional legal notification and reporting obligations to the relevant authorities; this is not affected by this policy.

9. HANDLING OF REPORTS

We greatly value responsible reporting. Currently, the BOWE GROUP does not operate a bug bounty program and does not provide financial compensation for vulnerability reports.

10. DATA PROTECTION

Personal data transmitted in connection with a vulnerability report will be used exclusively for the purpose of processing the report.

Processing is carried out in accordance with applicable data protection regulations, in particular the General Data Protection Regulation (GDPR).

The data will be made available only to those involved in the investigation and will be deleted or archived upon completion of the process in accordance with our internal retention policies.

For more information on the processing of personal data, please see our Privacy Policy under Privacy.