BLH Nobel Coordinated Vulnerability Disclosure Policy

BLH Nobel takes the security of our products and services seriously. We encourage customers, security researchers, and other parties to report potential security vulnerabilities to us so they can be investigated and addressed in a coordinated and responsible manner.

Please read this policy before reporting or testing a potential vulnerability.

Scope

This policy applies to potential cybersecurity vulnerabilities in BLH Nobel products and services. Vulnerabilities in third-party components may also be reported if they affect a BLH Nobel product.

For products that have reached the end of their support lifecycle, BLH Nobel may be unable to provide a software or firmware update. In such cases, we may provide recommendations or other risk-reducing measures.

Out of Scope

This policy does not cover:

- Products or services owned or controlled by third parties,
- Systems operated by customers, distributors, or other third parties,
- General technical support requests,
- Product defects without a cybersecurity impact,
- Warranty claims or product complaints,
- Ongoing security incidents, fraud, or phishing attempts,
- Unverified results from automated vulnerability scanners.

Reporting a Vulnerability

Potential vulnerabilities should be reported to:

Email: service.se@VPGSensors.com

Please use the following email subject:

Vulnerability report: [Product or service name]

Your report should include as much of the following information as possible:

- Product or service name,
- Product model and affected version,
- Firmware or software version,
- Description of the potential vulnerability,
- Steps required to reproduce the issue,
- Potential impact,
- Proof of concept, logs, or screenshots, if available,
- Your contact information.

Sensitive information should be encrypted before being submitted. Please do not include unnecessary personal data, customer data, passwords, private keys, or other confidential information.

Anonymous reports are accepted. However, if no contact information is provided, BLH Nobel will be unable to request additional information or provide status updates.

Analysis and Handling

After receiving a vulnerability report, BLH Nobel will:

1. Acknowledge receipt of the report and request additional information where necessary.
2. Review the information and attempt to reproduce the issue.
3. Assess the severity and potential impact.
4. Determine appropriate corrective or risk-reducing actions.
5. Coordinate with affected suppliers or other parties when necessary.
6. Keep the reporter informed of significant progress, where possible.

The time required to investigate and resolve a vulnerability depends on its complexity, potential impact, product lifecycle status, necessary verification activities, and involvement of third-party components.

For industrial products, additional testing or validation may be required before an update can be released.

Responsible Security Research

When investigating a potential vulnerability, you must:

- Comply with applicable laws and regulations.
- Limit testing to what is necessary to confirm the vulnerability.
- Avoid disruption of products, services, and industrial processes.
- Avoid affecting the safety of people, property, or the environment.
- Protect personal, customer, and confidential information.
- Stop testing immediately if sensitive information or safety-critical functions are accessed.
- Report the vulnerability to BLH Nobel without unnecessary delay.
- Allow BLH Nobel reasonable time to investigate and address the issue before public disclosure.

The following activities are not permitted:

- Denial-of-service or high-intensity testing.
- Testing of customer production environments without explicit permission.
- Manipulation of measurements, control signals, alarms, or safety functions in operational installations.
- Modification, deletion, or extraction of data.
- Establishing persistent access.
- Installing malware.
- Social engineering or physical security testing.
- Accessing other users’ accounts.
- Using stolen or unauthorized credentials.

Testing should preferably be performed in a controlled environment using equipment and systems that the researcher is authorized to test.

Coordinated Disclosure

We ask reporters of vulnerabilities not to publicly disclose information about a vulnerability before BLH Nobel has had reasonable time to investigate and address the issue.

BLH Nobel and the reporter of the vulnerabilities should, where possible, agree on the timing and level of detail of any public disclosure. Additional time may be required when a vulnerability:

- Affects safety-critical or industrial systems
- Requires extensive verification or validation
- Involves multiple suppliers or third-party components
- Requires customers to plan and implement an update
- Could create a significant risk if disclosed prematurely

When appropriate, BLH Nobel may publish a Security Advisory describing the affected products, potential impact, available updates, and recommended protective measures.

Recognition

With the reporter's consent, BLH Nobel may acknowledge individuals or organizations that responsibly report a valid and previously unknown vulnerability.

Contact

For questions regarding this policy or to report a potential vulnerability, contact:

service.se@VPGSensors.com

For general product support, warranty claims, or product complaints, please use BLH Nobel's regular support channels.

---

revision: R00
Publication date: 2026-09-10
Last updated: 2026-09-21