Coordinated Vulnerability Disclosure Policy

1. Purpose and Status of this Policy

Belimo is committed to the security of its products with digital elements and to responsible, transparent, and legally compliant handling of vulnerability reports.

This Coordinated Vulnerability Disclosure Policy ("Policy") describes how external and internal parties shall report suspected vulnerabilities relating to Belimo products with digital elements, how Belimo will assess and handle such reports, and the conditions under which Belimo supports good-faith security research.

This Policy is intended to support Belimo's vulnerability handling processes and coordinated vulnerability disclosure practices in alignment with applicable law, including Regulation (EU) 2024/2847 (Cyber Resilience Act, "CRA"), and recognised good practices for product security incident response and coordinated disclosure. It also supports Belimo's broader product cybersecurity governance.

For the avoidance of doubt, this Policy is a public-facing policy for reporting and coordination. It does not replace Belimo's internal incident response, crisis management, product safety, regulatory reporting, or remediation procedures. Where a report received under this Policy indicates an actively exploited vulnerability or a severe incident affecting the security of a product with digital elements, Belimo will assess and handle the matter in accordance with its internal regulatory escalation procedures, including, where applicable, reporting obligations under Art. 14 CRA.

Version	Date	Changes
1.0	20.08.2026	New

2. Who May Report

Belimo welcomes reports submitted in good faith by any person or entity, including, without limitation:

- security researchers
- customers and end users
- distributors, integrators, and business partners
- suppliers and service providers
- public authorities, CSIRTs, and other trusted intermediaries
- Belimo employees

Reports may also be submitted anonymously. However, anonymous reporting may limit Belimo's ability to request clarification, provide status updates, or coordinate disclosure.

3. Scope

3.1 In Scope

This Policy applies to suspected cybersecurity vulnerabilities affecting products with digital elements developed, manufactured, or placed on the market by Belimo, including, where relevant, associated remote data processing solutions for which Belimo is responsible.

- Without limitation, this may include:
- software vulnerabilities
- firmware vulnerabilities
- insecure default configurations
- authentication, authorization, session management, or cryptographic weaknesses
- vulnerabilities affecting confidentiality, integrity, availability, authenticity, or access control
- product-related issues that may indicate active exploitation
- vulnerabilities in third-party components integrated into Belimo products, where Belimo is the appropriate initial point of contact for coordination

3.2 Out of Scope

Unless Belimo expressly states otherwise, this Policy does not apply to:

- third-party products, software, or cloud services not developed or provided by Belimo
- Belimo corporate IT systems unrelated to products with digital elements
- general customer support requests, feature requests, or quality complaints that do not involve a security weakness
- purely physical safety or physical tampering issues, except to the extent they directly affect the cybersecurity of a product with digital elements
- social engineering, phishing simulations, spam campaigns, or testing directed at Belimo personnel or customers unless expressly authorized in writing

If a report falls outside the scope of this Policy, Belimo may, at its discretion, redirect it to another appropriate internal process.

4. Definitions

For the purposes of this Policy:

Vulnerability means a weakness, susceptibility, or flaw in a product with digital elements that may be exploited by a cyber threat.

Actively exploited vulnerability means a vulnerability for which there is reliable evidence that a malicious actor has exploited it within a system without the system owner's permission.

Severe incident means an incident having an impact on the security of a product with digital elements and meeting the applicable legal threshold under the CRA.

Reporter means any natural or legal person submitting a report under this Policy.

Coordinated vulnerability disclosure means a process in which vulnerability information is reported and handled in a cooperative and controlled manner to support validation, remediation, risk reduction, and, where appropriate, public disclosure.

Security advisory means a notice published by Belimo to inform users and other stakeholders of a vulnerability, its mitigation, a fix, or related security-relevant information.

5. How to Report

Belimo provides the following channels for reporting suspected vulnerabilities:

5.1 Preferred Reporting Channels

PSIRT email: psirt@belimo.com
PGP/GPG key for encrypted email: https://www.belimo.com/mam/corporate-communications/web/Product_PGP_Public_Key.asc

Belimo encourages the use of encrypted channels for sensitive vulnerability information.

5.2 What to Include in a Report

To support efficient triage and remediation, Belimo encourages reporters to provide, where available:

- product name and affected component
- product version, firmware version, software version, hardware model, and configuration details
- a clear description of the suspected vulnerability
- steps to reproduce the issue
- proof-of-concept material sufficient for validation
- logs, traces, screenshots, packet captures, or other technical evidence where relevant
- the suspected or observed impact
- whether exploitation is known or suspected
- the reporter's name, alias, or handle (e.g. GitHub or other professional identifiers) and contact details, unless the report is submitted anonymously
- whether the reporter has shared the issue with any third party, coordinator, or public authority

Belimo may request additional information where reasonably necessary to validate and assess the report.

6. Belimo's Commitments

Belimo will make reasonable efforts to handle reports submitted under this Policy promptly, professionally, and in good faith.

6.1 Acknowledgement

Belimo will aim to acknowledge receipt of a vulnerability report without undue delay.

6.2 Validation and Triage

Belimo will assess whether the report appears credible, in scope, reproducible, and security-relevant. This may include severity assessment, impact analysis, product applicability analysis, and internal escalation to the relevant technical, product, legal, and compliance stakeholders.

Submission of a report does not mean that Belimo confirms the existence of a vulnerability or agrees with the reporter's characterization of severity or impact.

6.3 Communication with the Reporter

Where contact details are available, Belimo will use reasonable efforts to keep the reporter informed about the status of the report, including, where appropriate:

- whether the report has been received
- whether it is in scope
- whether additional information is needed

Whether the issue has been validated and the remediation planning is underway
Belimo may limit the level of detail shared where necessary to protect security, confidentiality, legal privilege, personal data, trade secrets, or law enforcement interests.

6.4 Remediation

Where Belimo validates a vulnerability, it will determine and coordinate appropriate corrective action based on risk, severity, exploitability, technical feasibility, product lifecycle considerations, and legal obligations.

Corrective action may include, for example:

- a security patch
- a configuration change
- a mitigation or workaround
- additional monitoring or detection measures
- customer or partner communication
- a security advisory

6.5 Coordinated Disclosure

Belimo supports coordinated disclosure and will seek to coordinate disclosure timing with the reporter where appropriate.

Belimo's objective is to reduce risk to users and other stakeholders by allowing a reasonable opportunity for validation, remediation, and user communication before public disclosure.

Belimo does not commit to a fixed remediation deadline for all reports, since timing depends on the nature of the issue, exploitability, product complexity, supply chain dependencies, and the availability of safe corrective measures.

6.6 Security Advisories and User Information

Where appropriate, Belimo may publish a security advisory or otherwise inform affected users, customers, partners, or authorities.

A security advisory may include, as appropriate:

- affected products or versions
- a summary of the vulnerability and its impact
- severity information
- mitigations or workarounds
- fixed versions or corrective measures
- implementation guidance for users
- acknowledgment of the reporter, where agreed

7. Good-Faith Security Research and Safe Harbor

Belimo values good-faith security research that helps improve the security of its products.

Subject to applicable law, Belimo will not initiate legal action solely on the basis of security research activities that are conducted in good faith, consistent with this Policy, and intended to identify and responsibly report vulnerabilities.

For the purposes of this Policy, security research will generally be regarded as conducted in good faith only if the reporter:

- acts with the intention of promoting product security and reducing risk
- avoids privacy violations, unnecessary access to data, destruction of data, and service disruption
- does not exploit the issue beyond what is reasonably necessary to demonstrate the vulnerability
- does not exfiltrate, alter, or retain data beyond what is strictly necessary for proof of concept
- does not establish persistence, deploy malware, or pivot to other systems
- does not test systems, users, accounts, or environments that are outside the permitted scope
- does not engage in social engineering, phishing, extortion, or coercion
- gives Belimo a reasonable opportunity to validate and address the issue before public disclosure
- complies with applicable law and the rights of third parties

This Policy does not authorize any activity that is unlawful, that causes harm to Belimo, its customers, its partners, or other third parties, or that breaches contractual, regulatory, or statutory obligations.

Nothing in this Policy constitutes a waiver of legal rights in cases involving bad faith, unlawful conduct, abuse, data theft, service disruption, extortion, or any other conduct exceeding the bounds of responsible security research.

8. Regulatory Escalation and CRA Reporting

Belimo maintains internal procedures to assess whether information received under this Policy triggers legal or regulatory obligations.

Where Belimo becomes aware that a reported issue may constitute:

- an actively exploited vulnerability; or
- a severe incident having an impact on the security of a product with digital elements,

Belimo will assess the matter under its internal regulatory escalation procedures and, where applicable, comply with statutory notification and reporting obligations, including those under Art. 14 CRA.

This includes, where legally required, notification to the relevant CSIRT designated as coordinator and to ENISA via the applicable reporting platform within the timeframes laid down by law.

Nothing in this Policy should be understood as limiting or replacing Belimo’s internal legal assessment of whether a given set of facts meets the legal threshold for regulatory reporting.

9. Coordination with Suppliers and Third Parties

Where reasonably necessary for validation, remediation, or coordinated disclosure, Belimo may share relevant information with affiliated companies, suppliers, service providers, component manufacturers, external advisors, testing providers, coordinators, CSIRTs, and competent authorities.

Belimo will do so on a need-to-know basis and subject to appropriate confidentiality, legal, and security safeguards.

10. Confidentiality and Personal Data

Belimo will handle vulnerability reports with appropriate confidentiality and will process personal data contained in such reports in accordance with applicable data protection law.

Reporters should avoid including personal data or confidential third-party information unless it is reasonably necessary to understand and validate the issue.

11. No Reward Program Unless Expressly Announced

Unless Belimo expressly announces a separate vulnerability reward or bug bounty program, submission of a report under this Policy does not create any entitlement to payment, compensation, reimbursement, or public recognition.

12. Governance

This Policy is owned by Belimo's Product Security Incident Response Team (PSIRT), in coordination with the relevant product, engineering, legal, compliance, and cybersecurity functions.

If required, Belimo may update this Policy to reflect operational experience, legal developments, regulatory guidance, changes in reporting channels, or evolving best practices.

The current version of this Policy will be published on Belimo's security page.

13. Contact

For vulnerability reports and questions regarding this Policy, please contact:

Belimo PSIRT
psirt@belimo.com
https://www.belimo.com/about/belimo/productsecurity

For additional information:

Belimo Contact
https://www.belimo.com/ch/en_GB/contact/channels/belimo-contacts

14. Publication and Related Resources

Related resources may include:

- Belimo Security Page: https://www.belimo.com/about/belimo/productsecurity
- Belimo security.txt: https://www.belimo.com/.well-known/security.txt
- **PGP/GPG key for encrypted email:** https://www.belimo.com/mam/corporate-communications/web/Product_PGP_Public_Key.asc
- PGP/GPG Public Key Fingerprint: 386EF60BDD8DE4EC7D851D201A0D6C2DF51EB357