Coordinated Vulnerability Disclosure (CVD) Policy
Guideline for the Coordinated Disclosure of Vulnerabilities

1. Purpose
Bausch+Ströbel SE + Co. KG ("Bausch+Ströbel") is committed to the responsible, timely, and coordinated handling of security vulnerabilities affecting its products and digital services.
This Coordinated Vulnerability Disclosure (CVD) Guideline defines the process for reporting, assessing, validating, remediating, and disclosing vulnerabilities.

This policy is based on the requirements of:
- Cyber Resilience Act (EU) 2024/2847
- BSI TR-03183 Part 3 (Vulnerability Reports and Notifications)

2. Scope
This policy applies to all products with digital elements (hereinafter referred to as "products") and digital services provided by Bausch+Ströbel, including:
- Machinery and software products
- Digital services, cloud-based services, and remote solutions

This policy does not apply to:
- Security vulnerabilities in third-party products or services that are outside the control of Bausch+Ströbel
- Physical attacks or incidents that are not related to cybersecurity

3. Reporting vulnerabilities
Security vulnerabilities can be reported via:

email (preferred, encrypted): psirt@bausch-stroebel.com

Contact details are available on the following company website:
https://www.bausch-stroebel.com/de/unternehmen/security-advisories-psirt

Further contact details are available in the publicly available security.txt file:
https://www.bausch-stroebel.com/.well-known/security.txt

4. What counts as a valid vulnerability?
A vulnerability is considered valid if it:
- affects one of our products or services, and
- Has the potential to compromise confidentiality, integrity, availability, authenticity, non-repudiation, or reliability

The following, for example, are not considered valid vulnerabilities:
- Results of automated scans without context or supporting evidence.
- Configuration errors that are outside the responsibility of Bausch+Ströbel

5. Information to include
To enable efficient processing of the report, the following information should be included:
- Product name and affected version
- A detailed description of the security vulnerability
- Steps to reproduce the issue (proof of concept)
- Potential impact (e.g. Remote Code Execution)

6. Code of practice (Safe Harbor)

If you comply with the following rules, Bausch+Ströbel will not pursue legal action against you:

+ Do not exploit vulnerabilities (e.g. do not access confidential data or modify systems)
+ Do not carry out denial-of-service (DoS) attacks or social engineering tests against Bausch+Ströbel or its employees
+ Do not disclose information about the vulnerability to third parties until Bausch+Ströbel has addressed the vulnerability (coordinated disclosure)
+ Always act in good faith and comply with all applicable laws and regulations

7. Assurances from Bausch+Ströbel

Bausch+Ströbel provides the following assurances to individuals reporting vulnerabilities:

+ Confidential handling of reports (to the extent permitted by law)
+ No legal action will be taken against individuals who report vulnerabilities in good faith This assurance does not apply where there is clear evidence of criminal or malicious intent or activity
+ No requirement to sign a Non-Disclosure Agreement (NDA)
+ Recommendations and support for encrypted communication
+ A dedicated point of contact throughout the CVD process
+ Commitment to addressing reported vulnerabilities as quickly as possible

8. CVD process flow

1) Receipt and registration of the vulnerability report
2) Validation of the reported vulnerability
3) Risk assessment (e.g. CVSS score and exploitability assessment)
4) Remediation or mitigation of the vulnerability
5) Notification of affected users, where applicable
6) Coordinated disclosure

In the case of actively exploited vulnerabilities, Bausch+Ströbel will coordinate with the relevant national CSIRT (in Germany, this is CERT-Bund at the BSI).

9. Response times

Bausch+Ströbel is committed to the following response times:
≤ 5 business days: initial substantive response
≤ 10 business days: technical assessment or status update
These responses are non-automated

10. Disclosure & notification

+ Vulnerabilities that can be remediated will be addressed through security updates
+ Affected users will be notified without undue delay
+ Security information will be published in the form of security advisories
+ Security advisories will, where possible, be published in a machine-readable format using the Common Security Advisory Framework (CSAF)

Public disclosure will generally take place within 90 days, unless security considerations require a different disclosure timeline

11. Completion of the CDV process

A CVD process is considered complete when:

- a security update or mitigation has been released and
- affected users have been notified; or
- the reported vulnerability has been determined to be unfounded

12. Contact details & updates

The Product Security Incident Response Team (PSIRT) can be contacted via:
email (preferred, encrypted): psirt@bausch-stroebel.com

This policy will be reviewed at least once a year and updated as needed.