RICHTLINIE ZUR KOORDINIERTE OFFENLEGUNG VON SICHERHEITSLÜCKEN (CVD)

Dokument-Metadaten

Dokument-ID	sabo_de_cvd.docx
Titel	CVD Richtlinie
Version	1.00a
Klassifizierung	Öffentlich
Geltungsbereich	Eigens hergestellte und in Verkehr gebrachte Produkte mit digitalen Elementen oder Dienste
Erstellt am	22.06.2026
Nächste Prüfung	22.06.2029
Freigegeben durch	Dr.-Ing. U. Grünebaum
Status	Freigegeben

SABO Elektronik GmbH
Lohbachstr. 14
58239 Schwerte
Tel. 02304 / 97102 - 0

E-Mail: info@sabo.de
Internet: https://www.sabo.de/

Inhalt

1. Ziel und Geltungsbereich

Diese Richtlinie beschreibt, wie SABO Elektronik GmbH mit Meldungen über Sicherheitslücken umgeht und wie externe Sicherheitsforscher, Kunden oder Partner verantwortungsvoll Schwachstellen melden können. Ziel ist es, die Sicherheit unserer Produkte und Dienste kontinuierlich zu verbessern und Risiken für unsere Nutzer und Kunden zu minimieren.

Geltungsbereich

Diese Richtlinie gilt für die aktuellen, von uns hergestellten und in Verkehr gebrachten:

- Produkte mit digitalen Elementen
- Software-Komponenten
- interne und externe APIs

Inkrafttreten

Diese Richtlinie tritt am 01.09.2026 in Kraft und wird dreijährlich überprüft.

2. Vertraulichkeit und Datenschutz

Alle eingereichten Informationen werden vertraulich behandelt und ausschließlich zur Analyse und Behebung der Schwachstelle verwendet.

3. Kontakt für Sicherheitsmeldungen

Sicherheitslücken können gemeldet werden an:

Web:	https://www.sabo.de/security/
E-Mail:	psirt@sabo.de
PGP-Key:	https://www.sabo.de/security/pgp

Wir bestätigen den Eingang jeder Meldung innerhalb von maximal 72 Stunden.

4. Erwartung an meldende Personen oder Stellen

Wir bitten Sicherheitsforscher, folgende Grundsätze einzuhalten:

- Keine Ausnutzung der Schwachstelle über das notwendige Maß hinaus
- Keine Unterbrechung von Diensten oder Systemen
- Keine Manipulation oder Löschung von Daten
- Keine Weitergabe vertraulicher Informationen
- Verantwortungsvolle Offenlegung. Keine Veröffentlichung vor Patch oder Freigabe durch uns (Vermeidung von Zero-Day Situationen)

5. Unser Versprechen an Sicherheitsforscher

Wir verpflichten uns:

- keinen rechtlichen Schritte einzuleiten, solange verantwortungsvoll gehandelt wurde
- zu zeitnaher Rückmeldung zum Status der Meldung
- zu transparenter Kommunikation über Fortschritt und geplante Maßnahmen
- zu öffentlicher Anerkennung (Hall-of-Fame), sofern gewünscht

6. Erforderliche Informationen

- Beschreibung der Sicherheitslücke
- Betroffenes Produkt, möglichst mit Seriennummer und Firmware-Ständen
- Anleitung mit der die Lücke reproduzierbar nachzustellen ist
- Proof-of-Concept Code, falls vorhanden
- Netzwerk Trace, falls vorhanden

7. Ablauf nach Eingang einer Meldung

Unsere interne PSIRT-Richtlinie definiert den folgenden Ablauf wie folgt:

- Eingangsbestätigung innerhalb von 72 Stunden
- Triage & Bewertung
- Analyse & Reproduktion
- Fix-Entwicklung durch Engineering
- Patch-Release & Advisory (z. B. CSAF)
- Koordinierte Veröffentlichung mit dem Meldendem
- Regelmäßiger Kontakt mit der meldenden Person, um über den Stand zu informieren

8. Offenlegungszeitraum

Gemäß unserer internen PSIRT-Richtlinie, streben wir an, Schwachstellen innerhalb von 30 Tagen zu beheben. In kritischen Fällen erfolgt ein beschleunigter Prozess.

9. Anhang

Versionsverlauf

Revision	Datum	Seiten	Grund	Autor
1.00a	22.06.2026	1 - 5	Erstellung der ersten Version	D. Mika