Coordinated Vulnerability Disclosure Policy –

Fritz Husemann GmbH & Co. KG

Geltungsbereich

Diese Policy gilt für Sicherheitslücken in folgenden Produkten der Fritz Husemann GmbH & Co. KG:

- **E3CON - Das Energie Transparenz System** (Energiemonitoring nach ISO 50001)
- **Husemann INSIGHT** (Monitoring-Tool für elektrische Infrastruktur)
- **Husemann SmartPanel 4.0** (HSP, Zentrales Messdatenmanagement)
- **Husemann EDGE** (EDGE-Computing, Erfassungsmodul)
- **Husemann CONNECT** (MSP Fernwirktechnik)

Wie Sie eine Schwachstelle melden

Folgende Kontaktmöglichkeiten stehen Ihnen für die Meldung zur Verfügung:

- Erste Kontaktadresse: **psirt@husemann.de**
- Zweite Kontaktadresse: **nis2@husemann.de**
- Website-Formular: **www.husemann.de/security**

Ihre Meldung sollte enthalten:

- Betroffenes Produkt und Versions-/Firmwarestand
- Beschreibung der Schwachstelle und möglicher Auswirkungen
- Schritte zur Reproduktion, falls vorhanden
- Ihre Kontaktdaten für Rückfragen

Was Sie von uns erwarten können

- Eingangsbestätigung innerhalb von **3 Werktagen**
- Erste Einschätzung/Priorisierung innerhalb von **10 Werktagen**
- Laufende Information über den Bearbeitungsstand

Verantwortungsvolle Offenlegung

Wir bitten um eine koordinierte Offenlegungsfrist von in der Regel **90 Tagen** ab Bestätigung, bevor Details veröffentlicht werden. Bei aktiv ausgenutzten

Schwachstellen kann diese Frist kürzer
ausfallen. Den genauen Zeitpunkt der Veröffentlichung stimmen wir im Dialog mit Ihnen ab.

Safe Harbor

Wer diese Policy in gutem Glauben befolgt, handelt nach unserem Verständnis nicht rechtswidrig. Wir leiten keine rechtlichen Schritte gegen gutgläubige, verantwortungsvolle Sicherheitsforschung im Rahmen dieser Policy ein.

Wichtig: keine Tests an produktiven Kundenanlagen

Tests dürfen **ausschließlich** in Laborumgebungen oder an eigens dafür bereitgestellten Testsystemen erfolgen – niemals an produktiven Anlagen bei Kunden. Denial-of-Service-Tests, physische Manipulation an Anlagen sowie Social Engineering gegenüber Mitarbeitenden oder Kunden sind nicht Teil dieser Policy und werden nicht toleriert.

Rechtlicher Rahmen

Diese Policy ergänzt unsere Pflichten aus der EU Cyber Resilience Act (Verordnung (EU) 2024/2847), insbesondere Anhang I Teil II (Schwachstellenmanagement-Anforderungen).

Stand: 11. September 2026