IFSYS GmbH · Am Weißen Kreuz 5 · D-97633 Großbardorf

# RICHTLINIE ZUR KOORDINIERTEN OFFENLEGUNG VON SICHERHEITSLÜCKEN (Coordinated Vulnerability Disclosure CVD)

IFSYS Integrated
Feeding Systems GmbH
Am Weißen Kreuz 5
D-97633 Großbardorf

Tel. +49 9766/940098-0
Fax +49 9766/940098-199
Mail contact@ifsys.com
Web www.ifsys.com

*Grundlage: Verordnung (EU) 2024/2847 (Cyber Resilience Act), ISO/IEC 29147, ISO/IEC 30111*

Diese Richtlinie regelt, wie IFSYS Integrated Feeding Systems GmbH mit der Meldung, Bewertung, Behebung und Veröffentlichung von Sicherheitslücken in seinen Produkten mit digitalen Elementen umgeht (Coordinated Vulnerability Disclosure, nachfolgend „CVD"). Sie richtet sich an Sicherheitsforscher, Kunden, Partner und sonstige Dritte, die eine potenzielle Schwachstelle identifizieren, und konkretisiert die Anforderungen aus Art. 13 und 14 der Verordnung (EU) 2024/2847 (Cyber Resilience Act) sowie die Vorgaben der Normen ISO/IEC 29147 und ISO/IEC 30111.

## 1. GELTUNGSBEREICH

### 1.1 Erfasste Produkte

Diese Richtlinie gilt für sämtliche von IFSYS Integrated Feeding Systems GmbH entwickelten, hergestellten oder unter eigenem Namen in Verkehr gebrachten Produkte mit digitalen Elementen, einschließlich Software, eingebetteter Systeme und vernetzter Baugruppen.

### 1.2 Abgrenzung: Test- und Erstmeldungsscope gegenüber Zulieferer-Komponenten

Für die aktive Sicherheitsüberprüfung durch externe Dritte (Penetrationstests, Schwachstellensuche) gilt ausschließlich der von IFSYS Integrated Feeding Systems GmbH selbst entwickelte und gefertigte Bestandteil eines Produkts als Prüfgegenstand. Komponenten, Bauteile oder Software Dritter, die in ein Produkt von IFSYS Integrated Feeding Systems GmbH integriert, jedoch nicht von [Unternehmen] selbst hergestellt werden (z. B. Feldbus-, Steuerungs- oder Netzwerkkomponenten), sind vom aktiven Testumfang dieser Richtlinie ausgenommen. Entsprechende Erstmeldungen sind an den jeweiligen Komponentenhersteller zu richten.

Unabhängig von dieser Abgrenzung des Testumfangs bleibt [Unternehmen] als Hersteller des Gesamtprodukts dafür verantwortlich, öffentlich bekannt werdende Schwachstellen in integrierten Zulieferer-Komponenten zu beobachten, deren Relevanz für die eigenen Produktlinien zu bewerten und betroffene Kunden im Rahmen eines Security Advisories zu informieren (vgl. Abschnitt 5). Diese Beobachtungspflicht ergibt sich unmittelbar aus Art. 13 CRA und besteht unabhängig davon, ob die Schwachstelle über den in dieser Richtlinie beschriebenen Meldeweg oder über eine Veröffentlichung des Komponentenherstellers bekannt wird.

Bestehen Zweifel, ob ein Sachverhalt in den Geltungsbereich dieser Richtlinie fällt, ist vor Beginn jeglicher Prüfhandlung Kontakt über die in Abschnitt 2 genannten Kanäle aufzunehmen.

## 2. MELDEWEG

Meldungen sind ausschließlich über die folgenden Kanäle einzureichen:

- Meldeformular: https://www.ifsys.com/fileadmin/user_upload/2026_CybersecurityFormular.pdf
- E-Mail: psirt@ifsys.com
- Seciruty.txt gemäß RFC 9116: https://www.ifsys.com/fileadmin/user_upload/security.txt

Eine anonyme Meldung ist zulässig; in diesem Fall entfällt jedoch die Möglichkeit von Rückfragen, sodass eine möglichst vollständige technische Dokumentation erforderlich ist. Eine Meldung sollte, soweit bekannt, mindestens folgende Angaben enthalten: das betroffene Produkt einschließlich Versionsstand, eine technische Beschreibung der Schwachstelle (betroffene Komponente, Schnittstelle, Parameter), nachvollziehbare Schritte zur Reproduktion, eine Einschätzung des Schweregrads (vorzugsweise als CVSS-Vektor) sowie gegebenenfalls bereits bekannte Gegenmaßnahmen.

## 3. Bearbeitung der Meldung

1. Eingangsbestätigung innerhalb von zwei Werktagen durch das zuständige Sicherheitsteam.
2. Prüfung auf Vollständigkeit, Plausibilität und Dopplung mit bereits vorliegenden Meldungen.
3. Technische Analyse in Zusammenarbeit mit den zuständigen Entwicklungs- und Qualitätsverantwortlichen sowie Bewertung der Kritikalität anhand eines anerkannten Bewertungsverfahrens (CVSS).
4. Regelmäßige, mindestens monatliche Information der meldenden Person über den Bearbeitungsstand bis zum Abschluss des Verfahrens.

## 4. Behebung und Fristen

Wird festgestellt, dass eine gemeldete Schwachstelle bereits aktiv ausgenutzt wird, erfolgt die Behebung mit höchster Priorität: [Unternehmen] stellt innerhalb von 14 Tagen ab Kenntnisnahme entweder eine endgültige Abhilfemaßnahme oder eine wirksame risikomindernde Zwischenlösung bereit.

Für alle übrigen Schwachstellen strebt IFSYS Integrated Feeding Systems GmbH die Bereitstellung eines Patches oder einer wirksamen Risikominderung innerhalb von 90 Kalendertagen an. Der Lauf dieser Frist beginnt mit dem Zeitpunkt, zu dem [Unternehmen] die Meldung als valide Sicherheitslücke bestätigt hat, nicht mit dem Zeitpunkt des Eingangs der Meldung. Sind an der Behebung weitere Parteien beteiligt (z. B. Komponentenhersteller, externe Koordinierungsstellen), kann sich dieser Zeitraum verlängern; IFSYS Integrated Feeding Systems GmbH informiert die meldende Person in diesem Fall über den aktualisierten Zeitplan.

Bei aktiv ausgenutzten Schwachstellen gelten zusätzlich die gesetzlichen Meldepflichten des Cyber Resilience Act gegenüber ENISA und dem zuständigen nationalen CSIRT: eine Frühwarnung innerhalb von 24 Stunden, eine ausführlichere Meldung innerhalb von 72 Stunden sowie ein Abschlussbericht innerhalb von 14 Tagen nach Bereitstellung der Abhilfemaßnahme.

## 5. Veröffentlichung

Nach Bereitstellung einer Abhilfemaßnahme oder einer wirksamen Zwischenlösung veröffentlicht IFSYS Integrated Feeding Systems GmbH ein Security Advisory, das die betroffenen Produkte und Versionen, den Schweregrad sowie die empfohlenen Maßnahmen beschreibt. Details zu einer Schwachstelle werden bis zu diesem Zeitpunkt vertraulich behandelt. Betrifft die Meldung eine in ein Produkt von IFSYS Integrated Feeding Systems GmbH integrierte Zulieferer-Komponente, prüft IFSYS Integrated Feeding Systems GmbH die Relevanz für die eigenen Produktlinien und informiert betroffene Kunden entsprechend, auch wenn die Behebung durch den Komponentenhersteller erfolgt.

## 6. Ausgeschlossene, nicht qualifizierende Meldungen

Die folgenden Sachverhalte begründen für sich genommen keine Schwachstelle im Sinne dieser Richtlinie und werden entsprechend nicht priorisiert bearbeitet, auch wenn eine Meldung hierzu entgegengenommen wird:

- das Fehlen von HTTP-Sicherheitsheadern, die von aktuellen Browsern nicht mehr ausgewertet werden oder als veraltet gelten,
- clientseitige Fehlkonfigurationen außerhalb des Einflussbereichs von IFSYS Integrated Feeding Systems GmbH (z. B. eine unsichere Browsereinstellung der meldenden Person),
- unaufbereitete Rohausgaben automatisierter Schwachstellen-Scanner ohne eigene Analyse oder Reproduktionsnachweis.

## 7. Verhaltensanforderungen bei eigenen Prüfhandlungen

Wer im Rahmen dieser Richtlinie eigene Prüfhandlungen vornimmt, hat sich auf den in Abschnitt 1 beschriebenen Geltungsbereich zu beschränken und Handlungen zu unterlassen, die die Verfügbarkeit von Systemen beeinträchtigen, Daten verändern oder löschen, Sicherheitsmaßnahmen umgehen oder gegen geltendes Recht verstoßen; hierzu zählen insbesondere Denial-of-Service-Angriffe, Brute-Force-Versuche, Social Engineering, das physische Umgehen von Zutrittskontrollen sowie das Ausführen von Schadcode. Erlangte Daten sind auf das für den Nachweis erforderliche Minimum zu beschränken und dürfen nicht an Dritte weitergegeben werden. Eine Offenlegung gegenüber der Öffentlichkeit hat bis zum Abschluss des Verfahrens gemäß Abschnitt 5 zu unterbleiben.

## 8. Datenschutz und Vertraulichkeit

Personenbezogene Daten aus einer Meldung werden ausschließlich zur Bearbeitung des jeweiligen Falls gemäß den geltenden datenschutzrechtlichen Vorgaben verarbeitet. Eine Nennung der meldenden Person erfolgt ausschließlich mit deren vorheriger Zustimmung. Vertrauliche Meldungen können verschlüsselt über den in der security.txt hinterlegten Schlüssel übermittelt werden.

## 9. Änderungen dieser Richtlinie

IFSYS Integrated Feeding Systems GmbH behält sich vor, diese Richtlinie fortlaufend anzupassen. Maßgeblich ist stets die unter https://www.ifsys.com/fileadmin/user_upload/security.txt verlinkte, aktuelle Fassung.