wavecom

Connecting every...things

Kreative und innovative Lösungen im Bereich der Kommunikationstechnik.

Koordinierte Offenlegung von Schwachstellen

September 2026

Inhaltsverzeichnis

1. Dokumentenlenkung

> *EU 2024/2847 (CRA) — Art. 13 Abs. 8: Hersteller müssen über Konzepte und Verfahren zum Umgang mit Schwachstellen verfügen. Es muss ein Richtliniendokument bestehen, das versioniert ist, einen Verantwortlichen hat und regelmäßig überprüft wird.*

Feld	Wavecom
Name der Organisation	WAVECOM – Soluções Rádio, S.A.
Dokumenteneigner	Information Security Manager (ISM)
Sicherheitsteam	Wavecom Product Security Incident Response Team (PSIRT) — im Aufbau. Bis zur förmlichen Einrichtung wird die Funktion vom Information Security Manager gemeinsam mit der F&E-Abteilung wahrgenommen.
Version	1.0
Datum des Inkrafttretens	8. September 2026
Überprüfungszyklus	Jährlich oder früher bei einer wesentlichen Produktänderung oder einer Änderung des geltenden CRA-Rahmens
Klassifizierung	Öffentlich

2. Zweck

WAVECOM ist der Sicherheit der Produkte mit digitalen Elementen verpflichtet, die das Unternehmen in Verkehr bringt. Diese **Richtlinie zur koordinierten Offenlegung von Schwachstellen (CVD)** beschreibt, wie Dritte — darunter Sicherheitsforschende, Kunden und die Öffentlichkeit — mögliche Sicherheitsschwachstellen in unseren Produkten und Systemen melden können und wie wir mit diesen Meldungen umgehen.

Diese Richtlinie ist an der Verordnung (EU) 2024/2847 (Cyber Resilience Act — CRA) und an prEN 40000-1-3 ausgerichtet, die Anforderungen und Empfehlungen für Hersteller von Produkten mit digitalen Elementen zur Offenlegung möglicher Schwachstellen festlegt.

3. Rollen und Verantwortlichkeiten

> *EU 2024/2847 (CRA) — Art. 13 Abs. 17: Hersteller müssen eine zentrale Anlaufstelle benennen. Diese muss leicht auffindbar sein, den Nutzern die Wahl des bevorzugten Kommunikationsmittels ermöglichen und darf sich nicht auf automatisierte Werkzeuge beschränken.*

3.1 Internes Sicherheitsteam

Das für die Offenlegung von Schwachstellen zuständige interne Team ist das Wavecom Product Security Incident Response Team (PSIRT). Ihm obliegt:

Entgegennahme und Bestätigung gemeldeter Schwachstellen.

Validierung, Bewertung und risikobasierte Priorisierung der Schwachstellen.

Koordinierung der Behebungsmaßnahmen mit den betroffenen internen Teams.

Steuerung der Kommunikation während des gesamten Bearbeitungsprozesses.

Herausgabe von Sicherheitshinweisen und Benachrichtigungen, soweit angebracht.

Feld	Wavecom
Für die Entgegennahme von Meldungen zuständiges Team bzw. zuständige Person	Information Security Manager (ISM) als zentrale Anlaufstelle nach CRA, mit Überwachung von ciberseguranca@wavecom.pt.
Besteht ein förmliches PSIRT?	Die Cybersicherheitsaufgaben sind derzeit auf das technische Team von Wavecom verteilt. Die Einrichtung eines eigenen PSIRT ist geplant.
Wer koordiniert die Behebung?	F&E-Abteilung gemeinsam mit dem Product Security Owner der betroffenen Produktlinie.
Wer genehmigt die Veröffentlichung?	Der Vorstand auf Vorschlag des ISM.

3.2 Was wir von Meldenden erwarten

Von jeder Person und Organisation, die eine Schwachstelle meldet, wird erwartet, dass sie nach Treu und Glauben handelt und Folgendes beachtet:

- Die Schwachstelle nicht über das zur Bestätigung ihres Vorliegens erforderliche Maß hinaus auszunutzen.
- Keine Daten über das zum Nachweis des Problems unbedingt erforderliche Maß hinaus abzurufen, zu verändern oder zu exfiltrieren.
- Die Schwachstelle nicht öffentlich zu machen, bevor wir angemessen Gelegenheit zur Untersuchung und Behebung hatten.
- Ausreichende Angaben bereitzustellen, damit wir das gemeldete Problem reproduzieren, bewerten und validieren können.
- Im Rahmen von Tests keine Denial-of-Service-Angriffe, kein Social Engineering und kein Phishing durchzuführen.

4. Geltungsbereich

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: Die Richtlinie zur Offenlegung von Schwachstellen sollte die sicheren Kommunikationswege, den Geltungsbereich, die Veröffentlichung, die Anerkennung und den Inhalt der Meldungen festlegen. EU 2024/2847 (CRA) — Anhang I Teil I Nummer 2 Buchstabe a: Produkte müssen ohne bekannte ausnutzbare Schwachstellen in Verkehr gebracht werden, was ein Verfahren zur Entgegennahme von Meldungen voraussetzt.*

4.1 Erfasste Produkte und Systeme

Die folgenden Systeme, Produkte und Dienste fallen in den Geltungsbereich dieser Richtlinie:

Produkt / System	Version / URL / Einzelheiten zum Umfang	Cloud / Anwendung enthalten?
Wavecom IoT Gateway	Baureihen WR, WK und WT — alle unterstützten Hardware-Revisionen und Firmware-Versionen, die auf dem EU-Markt bereitgestellt wurden, einschließlich der vor dem 11. September 2026 bereitgestellten Geräte (CRA Art. 69 Abs. 3). Betriebssystem auf der Hardware der Wavecom IoT Gateway WR-Serie — WaveOS — Versionen ab 2025.	Ja — Verwaltung über den Wavecom IoT Manager

Produkt / System	Version / URL / Einzelheiten zum Umfang	Cloud / Anwendung enthalten?
Wavecom IoT Manager	Zentrale Webplattform als SaaS und On-Premises — alle unterstützten Versionen, einschließlich: Dienst zur Verwaltung und Bereitstellung von Gateways; Dienst zur Verwaltung und Bereitstellung von Geräten; Dienst zur Flottenüberwachung; Dienst zur Wasserüberwachung.	Nein
Cloud Authentication System (CAS)	Dienst zur WLAN-Gastauthentifizierung und Zugangskontrolle, als SaaS und On-Premises, in die Plattform Wavecom IoT Manager integriert oder eigenständig betrieben.	Nein
WHERE IS®	RTLS- und RFID-Ortungsplattform einschließlich der von Wavecom entwickelten Softwarekomponenten, als SaaS und On-Premises; Hardware Dritter wird von deren jeweiligen Herstellern abgedeckt.	Nein

4.2 Nicht erfasst (außerhalb des Geltungsbereichs)

Folgendes fällt nicht in den Geltungsbereich dieser Richtlinie. Entsprechende Meldungen werden nicht untersucht:

- Produkte, Dienste oder Infrastrukturen Dritter, die nicht im Eigentum von Wavecom stehen oder von Wavecom betrieben werden.
- Social Engineering, Phishing oder Angriffe auf die physische Sicherheit von Wavecom oder ihren Beschäftigten.
- Denial-of-Service-Angriffe (DoS) und verteilte Denial-of-Service-Angriffe (DDoS).
- Produkte oder Softwareversionen, die das Ende ihrer Lebensdauer erreicht haben und nicht mehr unterstützt werden.
- Schwachstellen, die Wavecom bereits bekannt sind oder die bereits von Dritten gemeldet wurden.

5. Meldung einer Schwachstelle

> *EU 2024/2847 (CRA) — Art. 13 Abs. 17: Die zentrale Anlaufstelle muss leicht auffindbar sein, den Nutzern die Wahl des bevorzugten Kommunikationsmittels ermöglichen und darf sich nicht auf automatisierte Werkzeuge beschränken. prEN 40000-1-3 [PRE-2-RQ-02]: Es muss mindestens ein Kontaktmechanismus bestehen. [RCP-1-RQ-01]: Die Kontaktmechanismen müssen öffentlich zugänglich sein.*

5.1 Kontaktkanäle

Kanal	Erforderlich?	Einzelheiten
Sicherheits-E-Mail-Adresse	Erforderlich — überwachtes Postfach	ciberseguranca@wavecom.pt — überwachtes Postfach, betrieben vom Information Security Manager (ISM) als zentrale Anlaufstelle nach CRA gemäß Art. 13 Abs. 17. Eingangsbestätigung innerhalb von 3 bis 5 Arbeitstagen.
Telefon / Support	Optional — sinnvoll, wenn bereits eine Support-Hotline besteht	Der technische Support von Wavecom kann Meldungen über die üblichen Kundendienstkanäle entgegennehmen. Die Support- und Serviceteams sind angewiesen, jeden Hinweis auf eine Sicherheitsschwachstelle oder auf eine aktive Ausnutzung unverzüglich an ciberseguranca@wavecom.pt weiterzuleiten — bei Verdacht auf Ausnutzung zusätzlich telefonisch — und zwar ohne vorherige technische Bewertung.
PGP-Schlüssel für E-Mails	Empfohlen, wenn E-Mail der Hauptkanal ist — ermöglicht die sichere Übermittlung sensibler Informationen	Derzeit nicht veröffentlicht. Wer sensible Informationen übermitteln muss, fordert die Verschlüsselungsmodalitäten unter ciberseguranca@wavecom.pt an.

5.2 Inhalt der Meldung

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: Die Richtlinie sollte den erwarteten Inhalt von Schwachstellenmeldungen festlegen.*

Wir bitten darum, nach Möglichkeit mindestens die folgenden Angaben beizufügen; sie ermöglichen uns eine schnelle Triage und Untersuchung:

- Name, Modell, Version und/oder URL des betroffenen Produkts.
- Eine klare Beschreibung der Schwachstelle und ihrer möglichen Auswirkungen auf die Sicherheit.
- Eine Schritt-für-Schritt-Anleitung zur Reproduktion einschließlich der verwendeten Werkzeuge und Konfigurationen.
- Belege — Bildschirmfotos, Netzwerkmitschnitte, Protokolldateien oder Proof-of-Concept-Code.
- Eine Einschätzung des Schweregrads bzw. ein CVSS-Wert, sofern vorhanden (optional).
- Kontaktangaben für Rückfragen — anonyme Meldungen werden ebenfalls angenommen.

6. Umgang mit Schwachstellen

> *CRA / prEN 40000-1-3 [PRE-2-RQ-03]: Die Erwartungen an die Kommunikation mit der meldenden Person müssen beschrieben sein. EU 2024/2847 (CRA) — Anhang I Teil II Nummer 2: Schwachstellen müssen unverzüglich behandelt und behoben werden, auch durch Bereitstellung von Sicherheitsaktualisierungen.*

6.1 Eingangsbestätigung

> *CRA / prEN 40000-1-3 [RCP-1-RQ-02]: Jeder Meldung muss eine Vorgangsnummer zugewiesen werden. [RCP-1-RQ-03]: Die Eingangsbestätigung muss innerhalb der in dieser Richtlinie genannten Frist erfolgen.*

Nach Eingang einer möglichen Schwachstellenmeldung bestätigt Wavecom den Eingang innerhalb der nachstehend genannten Frist. Die Bestätigung enthält eine eindeutige Vorgangsnummer.

WAVECOM bestätigt den Eingang aller Schwachstellenmeldungen innerhalb von 3 bis 5 Arbeitstagen. Die Bestätigung enthält eine eindeutige Vorgangsnummer, die in der weiteren Korrespondenz anzugeben ist.

6.2 Triage und Verifizierung

> *CRA / prEN 40000-1-3 [VRF-1-RQ-01]: Enthält die ursprüngliche Meldung keine ausreichenden Angaben zur Reproduktion der Schwachstelle, ist die meldende Person zur Nachreichung weiterer Einzelheiten zu kontaktieren.*

Nach der Eingangsbestätigung bewertet das Sicherheitsteam die Meldung innerhalb der festgelegten Frist. Dabei nimmt Wavecom Folgendes vor:

- Validierung und Reproduktion der gemeldeten Schwachstellen.
- Bewertung des Schweregrads anhand eines etablierten Bewertungssystems (CVSS v3.1).
- Ermittlung der betroffenen Produkte und Versionen.
- Festlegung der Priorität und des für die Behebung Verantwortlichen.

Enthält die eingereichte Meldung keine ausreichenden Angaben zur Reproduktion der Schwachstelle, wendet sich das Sicherheitsteam an die meldende Person, um die erforderlichen zusätzlichen Einzelheiten anzufordern.

WAVECOM schließt die erste Triage ab und informiert die meldende Person innerhalb von 7 Arbeitstagen nach der Eingangsbestätigung über den Bearbeitungsstand. Betrifft die Meldung eine aktiv ausgenutzte Schwachstelle, beginnt die Triage unverzüglich und das Meldeverfahren nach Artikel 14 CRA wird parallel ausgelöst, unabhängig von der Kommunikation mit der meldenden Person.

6.3 Fristen für die Behebung

> *prEN 40000-1-3 [RMD-2-RQ-01]: Die Behebung muss entwickelt werden. [RMD-3-RQ-01]: Die Behebung muss getestet werden.*

WAVECOM strebt an, validierte Schwachstellen innerhalb der folgenden Zielfristen je nach Schweregrad zu beheben:

Schweregrad	Zielfrist
Kritisch / hoch (CVSS ≥ 7,0)	30 Kalendertage
Mittel (CVSS 4,0 – 6,9)	60 Kalendertage
Niedrig (CVSS < 4,0)	90 Kalendertage
Sonderfälle (soweit einschlägig)	Geräte im Feld, die nur in einem geplanten Wartungsfenster aktualisiert werden können, sowie Schwachstellen in Komponenten Dritter, für die eine Korrektur des Lieferanten aussteht. Verlängerte Fristen werden vorab mit der meldenden Person vereinbart, schriftlich begründet und dokumentiert.

Skala für Schweregrad und Reaktionszeiten

NIEDRIG	MITTEL	HOCH	KRITISCH
CVSS 0,1–3,9 Zielfrist: 90 Tage	CVSS 4,0–6,9 Zielfrist: 60 Tage	CVSS 7,0–8,9 Zielfrist: 30 Tage	CVSS 9,0–10,0 Zielfrist: 30 Tage*

** Kritische Schwachstellen, die aktiv ausgenutzt werden, werden für die schnellstmögliche Behebung vorrangig behandelt, auch vor der Zielfrist von 30 Tagen.*

Kann eine Korrektur nicht innerhalb der Zielfrist bereitgestellt werden, informiert Wavecom die meldende Person vorab über einen neuen Termin und, soweit vorhanden, über vorläufige Maßnahmen zur Risikominderung.

> *CRA / prEN 40000-1-3 [RMD-3-RQ-01]: Die Behebung muss vor der Freigabe getestet werden, um zu bestätigen, dass sie die Schwachstelle beseitigt und keine neuen Probleme verursacht.*

Vor der Freigabe einer Korrektur prüfen wir, dass diese die gemeldete Schwachstelle beseitigt und keine neuen Sicherheitslücken verursacht. Bei kritischem und hohem Schweregrad umfassen die Tests eine funktionale Verifizierung und, soweit angebracht, Regressionstests.

6.4 Koordinierte Veröffentlichung

Wir praktizieren die koordinierte Offenlegung: Sobald eine Korrektur vorliegt, stimmen wir mit der meldenden Person einen Termin für die Veröffentlichung der Informationen über die Schwachstelle ab.

> *CRA — Anhang I Teil II Nummer 4: Informationen über behobene Schwachstellen müssen öffentlich bekannt gemacht werden, einschließlich Beschreibung, betroffener Versionen, Schweregrad und Hinweisen zur Behebung. prEN 40000-1-3 [PRE-2-RC-02]: Die Richtlinie sollte Angaben zum Veröffentlichungsverfahren enthalten. [PRE-2-RC-03]: Die Offenlegung muss koordiniert erfolgen, um eine verfrühte Veröffentlichung zu vermeiden.*

WAVECOM strebt an, die koordinierte Offenlegung innerhalb von 90 Kalendertagen ab dem Datum der Eingangsbestätigung abzuschließen. Ist dies nicht möglich, kontaktieren wir die meldende Person vor Fristablauf, um einen neuen Termin zu vereinbaren.

Wichtig — Recht auf Offenlegung: Soweit dies zum Schutz der Nutzer oder zur Erfüllung geltender rechtlicher Pflichten erforderlich ist, behält sich **WAVECOM** das Recht vor, Informationen über die Schwachstelle ohne vorherige Zustimmung oder Beteiligung der meldenden Person zu veröffentlichen.

Vereinbaren beide Seiten eine Sperrfrist — einen Zeitraum, in dem keine Seite Informationen über die Schwachstelle veröffentlicht — so werden der vereinbarte Zeitraum und dessen Enddatum (Veröffentlichungstermin) schriftlich festgehalten. Jede Seite kann mit angemessener Begründung eine Verlängerung der Sperrfrist beantragen.

Nach Freigabe der Korrektur wird Wavecom:

- die meldende Person über die Behebung der Schwachstelle informieren;
- einen Sicherheitshinweis, eine Release Note oder eine Produktmitteilung veröffentlichen;
- die meldende Person mit deren Einverständnis im öffentlichen Hinweis nennen.

7. Zentrale Meldeplattform (SRP)

Weitere Informationen: Verordnung (EU) 2024/2847, EUR-Lex, Erwägungsgrund 65.

Begriffsbestimmungen

Aktiv ausgenutzte Schwachstelle: Sicherheitsvorfall, bei dem eine aktive Schwachstelle des Produkts von einem böswilligen Akteur ausgenutzt wird.

Schwerwiegender Sicherheitsvorfall: Sicherheitsvorfall, bei dem die Sicherheitsfunktionen des Produkts erheblich beeinträchtigt werden und der nicht als „aktiv ausgenutzte Schwachstelle“ einzustufen ist.

7.1 Mechanismen der Informationsgewinnung

Kanal	Definition	Einzelheiten
Kundenbefragungen	Kunden werden regelmäßig zu Sicherheitsvorfällen im Zusammenhang mit den Produkten befragt.	Verantwortlich: Vertriebsabteilung und technischer Support. Sicherheit ist Bestandteil der regelmäßigen Kundengespräche und der Einsätze vor Ort. Die Aufzeichnungen werden im Vorfallregister geführt; jeder Hinweis auf eine Ausnutzung wird unverzüglich an den ISM eskaliert.
Threat Intelligence	Auswertung kommerzieller und offener Quellen zu ausgenutzten Schwachstellen	Hinweise des CNCS und des CERT.PT, Veröffentlichungen der ENISA, CVE-Feeds im Abgleich mit dem Komponentenverzeichnis (SBOM) von WaveOS und der Plattformen (IoT Manager, CAS und WHERE IS) sowie Bulletins von Lieferanten und ODM/OEM-Partnern (RAK, Supermicro, Kontron, Quectel, SimCom und Cloud-Anbietern).
Eingereichte Schwachstellen	Bewertung der über die Meldekanäle eingegangenen Schwachstellen, um festzustellen, ob sie aktiv ausgenutzt werden.	Die unter ciberseguranca@wavecom.pt nach dieser Richtlinie eingehenden Meldungen werden vom ISM triagiert, der feststellt, ob belastbare Anhaltspunkte für eine aktive Ausnutzung vorliegen.

Kanal	Definition	Einzelheiten
Internes Schwachstellen-Management	Bewertung intern festgestellter Schwachstellen, um zu ermitteln, ob sie aktiv ausgenutzt werden	Erkenntnisse aus dem sicheren Entwicklungsprozess (SGSI_PLT10), aus internen und externen Tests sowie aus der Überwachung und Protokollauswertung der SaaS-Plattformen (IoT Manager, CAS, WHERE IS®) werden auf Anhaltspunkte für eine aktive Ausnutzung geprüft.
Sonstiges		Interne Eskalation: Jede beschäftigte Person, jeder Auftragnehmer und jeder Servicetechniker, der einen Hinweis auf eine aktive Ausnutzung erhält, meldet diesen unverzüglich schriftlich an den ISM — ohne vorherige technische Bewertung und ohne Filterung über den Dienstweg.

7.2 Meldungen an die ENISA

Die folgenden Meldungen werden über die zentrale Meldeplattform der ENISA übermittelt:

- https://portal.cra-srp.enisa.europa.eu/

Art der Meldung	Frist (ab Kenntnis)	Inhalt der Meldung
Frühwarnung	24 Std.	Art der Meldung (Schwachstelle / Vorfall) Meldestufe (24 Std., 72 Std., Abschluss) Name des Herstellers oder Verwalters Produkt Titel
Meldung der Schwachstelle / des Vorfalls	72 Std.	Inhalt der Frühwarnung Art der Schwachstelle Art der Ausnutzung Ergriffene Korrektur- oder Minderungsmaßnahmen Korrektur- oder Minderungsmaßnahmen, die Nutzer ergreifen können Vertraulichkeit der Informationen (soweit einschlägig)

Art der Meldung	Frist (ab Kenntnis)	Inhalt der Meldung
Abschlussbericht (Schwachstellen)	14 Tage	Inhalt der Meldung der Schwachstelle / des Vorfalls Datum der Verfügbarkeit der Korrektur- oder Minderungsmaßnahme Vollständige Beschreibung der Schwachstelle Schweregrad der Schwachstelle Auswirkungen der Schwachstelle Böswilliger Akteur, der die Schwachstelle ausgenutzt hat Einzelheiten zur Sicherheitsaktualisierung bzw. zu den verfügbaren Korrekturmaßnahmen
Abschlussbericht (schwerwiegende Vorfälle)	1 Monat	Inhalt der Meldung der Schwachstelle / des Vorfalls Ausführliche Beschreibung des Vorfalls Schweregrad des Vorfalls Auswirkungen des Vorfalls Art der Bedrohung bzw. Ursache des Vorfalls Ergriffene und laufende Minderungsmaßnahmen

8. Vertraulichkeit und anonyme Meldungen

> *prEN 40000-1-3 [PRE-5-RC-03]: Meldende müssen die Möglichkeit haben, Meldungen anonym einzureichen.*

Alle Schwachstellenmeldungen werden vertraulich behandelt. Von meldenden Personen bereitgestellte personenbezogene Daten werden ohne ausdrückliche Einwilligung nicht an Dritte weitergegeben, es sei denn, geltendes Recht schreibt dies vor.

Wer anonym bleiben möchte, kann Meldungen über jeden der genannten Kanäle ohne Angabe personenbezogener Daten einreichen. Zu beachten ist, dass Anonymität unsere Möglichkeiten einschränken kann, über den Bearbeitungsstand zu informieren oder eine förmliche Anerkennung auszusprechen.

Anonyme Meldungen werden angenommen und zu denselben Bedingungen triagiert wie namentlich eingereichte Meldungen. Ohne Kontaktangaben können wir jedoch keine Rückfragen stellen, keinen Termin für die koordinierte Offenlegung vereinbaren und nicht über den Bearbeitungsstand informieren.

9. Kontaktangaben

Feld	Einzelheiten
Sicherheitskontakt	ciberseguranca@wavecom.pt
Postanschrift	WAVECOM – Soluções Rádio, S.A. Rua das Cardadeiras, 107 3800-125 Aveiro, Portugal
Öffentlicher PGP-Schlüssel	Auf Anfrage erhältlich.
Erreichbarkeit	09:00–18:00 Uhr (Europa/Lissabon), Montag bis Freitag, ausgenommen portugiesische Feiertage. Meldungen mit Hinweisen auf eine aktive Ausnutzung werden außerhalb dieser Zeiten über den ständigen Eskalationskontakt weitergeleitet.
Eskalationskontakt	Information Security Manager (ISM) als zentrale Anlaufstelle nach CRA. Die Eskalationskontakte sind in SGSI_PLT19 (Liste der Behördenkontakte) dokumentiert.

10. Verwaltung der Richtlinie

10.1 Überprüfung und Aktualisierung

Diese Richtlinie wird mindestens jährlich überprüft, bei wesentlichen Änderungen des Produktprogramms, des Sicherheitsteams oder des regulatorischen Umfelds auch früher. Aktualisierte Fassungen werden auf der Website von Wavecom veröffentlicht und intern bekannt gemacht.

Feld	Wavecom
Wo wird diese Richtlinie veröffentlicht?	https://www.wavecom.pt/security (zu bestätigen), mit einer security.txt-Datei unter https://www.wavecom.pt/.well-known/security.txt und einem Verweis in der Produktdokumentation.
Wer ist für die Überprüfung verantwortlich?	Information Security Manager (ISM)
Nächste Überprüfung	September 2027 oder früher bei einer wesentlichen Produktänderung oder einer Änderung des geltenden CRA-Rahmens

10.2 Ausnahmen

Jede Ausnahme von dieser Richtlinie bedarf der Genehmigung des Dokumenteneigners und ist im Ausnahmeregister zu erfassen. Alle Ausnahmen sind befristet und werden jährlich überprüft.

11. Änderungsverzeichnis

Version	Datum	Autor	Beschreibung der Änderung
1.0	8. September 2026	Information Security Manager (ISM)	Erstfassung, abgeleitet von der CVD-Richtlinienvorlage von Eurofins v1.0