					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P39					Dokumenttitel: **Richtlinie zur koordinierten Offenlegung von Schwachstellen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
EU-DSGVO	Art. 32(1)(d)	
EU NIS2	Art. 21(2)(e)	
EU DORA	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Zweck

1.1 Es ist ein formaler Prozess für die Entgegennahme, Bearbeitung und Offenlegung von Informationen über Schwachstellen einzurichten, die die Systeme oder Dienste der Organisation betreffen, wie nach Artikel 21 Absatz 2 Buchstabe e NIS2 für die Behandlung und Offenlegung von Schwachstellen erforderlich.

1.2 Externe Sicherheitsforscher, Partner und Nutzer sind dazu anzuhalten, Schwachstellen verantwortungsvoll zu melden (Coordinated Vulnerability Disclosure, CVD). Zudem wird festgelegt, wie die Organisation Informationen über Schwachstellen an relevante Interessengruppen kommuniziert.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Netzwerk- und Informationssysteme, die sich im Eigentum der Organisation befinden oder von ihr betrieben werden, sowie für alle in diesen Systemen identifizierten Schwachstellen.

2.2 Sie gilt für interne Teams (Informationssicherheit, IT, Entwicklung) sowie für alle externen Parteien, die Schwachstellen melden (z. B. Forscher, Kunden, Lieferanten). Sie regelt außerdem die Kommunikation mit Produktherstellern oder Dienstleistern, sofern deren Komponenten von der Schwachstelle betroffen sind.

3. Ziele

3.1 Schwachstellen sind zeitnah zu identifizieren und zu beheben, indem sowohl interne Bewertungen als auch externe Meldungen genutzt werden.

3.2 Externen Meldenden sind klare Vorgaben bereitzustellen, damit sie Informationen über Schwachstellen sicher und rechtmäßig übermitteln können und die Organisation wirksam reagieren sowie Abhilfemaßnahmen umsetzen kann.

3.3 Die Einhaltung der Anforderungen der NIS2 sowie der branchenüblichen bewährten Verfahren (ISO/IEC 29147 und ISO/IEC 30111) zur koordinierten Offenlegung von Schwachstellen ist sicherzustellen, um die Sicherheit des gesamten Ökosystems zu verbessern.

4. Rollen und Verantwortlichkeiten

4.1 Vulnerability Response Team (VRT): Ein benanntes Team unter Leitung des CISO oder des für das Schwachstellenmanagement Verantwortlichen, das Meldungen zu Schwachstellen entgegennimmt, triagiert, Risiko und Auswirkungen bewertet sowie die Behebung und öffentliche Offenlegung koordiniert.

4.2 IT- und Entwicklungsteams: Arbeiten mit dem VRT zusammen, um gemeldete Schwachstellen zu validieren, Patches oder risikomindernde Maßnahmen zu entwickeln und zu testen sowie Korrekturen bereitzustellen. Sie stellen bei Bedarf technische Details für Sicherheitshinweise bereit.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Überwachung und Audit

9.1 Das VRT führt ein Offenlegungsprotokoll für Schwachstellen, in dem jede Meldung vom Eingang bis zum Abschluss nachverfolgt wird. Dieses Protokoll wird monatlich überprüft, um den fristgerechten Fortschritt offener Punkte sicherzustellen. Überfällige Punkte sind zu eskalieren.

9.2 Die interne Audit- und Compliance-Funktion oder ein externer Sicherheitsbewerter überprüft jährlich die Wirksamkeit des Prozesses zur Behandlung von Schwachstellen, z. B. indem Stichproben von Schwachstellenfällen daraufhin geprüft werden, ob sie gemäß dieser Richtlinie behandelt wurden (Eingangsbestätigung, Behebung, Offenlegung innerhalb angemessener Fristen). Zudem wird verifiziert, dass der öffentlich erreichbare Offenlegungskanal funktionsfähig ist (z. B. dass Test-E-Mails empfangen und bearbeitet werden).

9.3 Kennzahlen zu Schwachstellen (Anzahl nach Schweregrad, Zeiten zur Behebung usw.) werden vierteljährlich zusammengestellt und dem Governance-Gremium für Cybersicherheit vorgelegt, um Aktualisierungen der Risikobewertung zu unterstützen.

10. Überprüfung und Pflege

10.1 Diese Richtlinie wird mindestens jährlich überprüft. Zusätzlich löst jede wesentliche Änderung unserer IT-Umgebung (z. B. die Einführung eines neuen internetseitig erreichbaren Dienstes) oder relevante regulatorische Entwicklungen (z. B. neue EU-Vorschriften zur Offenlegung von Produktschwachstellen) eine außerplanmäßige Überprüfung aus.

10.2 Aktualisierungen dieser Richtlinie berücksichtigen Rückmeldungen externer Meldender sowie Erkenntnisse aus internen Analysen nach Vorfällen. Wesentliche Änderungen werden vom CISO genehmigt, an alle Mitarbeiter kommuniziert und aus Transparenzgründen in unserem Online-Richtlinienrepository für Informationssicherheit veröffentlicht.

11. Zugehörige Richtlinien und Verknüpfungen

11.1 P01 – Informationssicherheitsrichtlinie. Managementvorgabe für die Behandlung und Offenlegung von Schwachstellen.

11.2 P19 – Richtlinie zum Schwachstellen- und Patch-Management. Interne Prozesse zur Behebung mit Anbindung an den CVD-Eingang.

11.3 P24 – Richtlinie für sichere Softwareentwicklung. Führt Korrekturen und Härtungsmaßnahmen im Software Development Life Cycle (SDLC) aus gemeldeten Sachverhalten zusammen.

11.4 P25 – Richtlinie zu Anforderungen an die Anwendungssicherheit. Stellt sicher, dass Produkte über offenlegungsfähige Sicherheitsanforderungen verfügen.

11.5 P30 – Incident-Response-Richtlinie. Behandelt die aktive Ausnutzung offengelegter Schwachstellen.

11.6 P31 – Richtlinie zur Beweissicherung und Forensik. Bewahrt Artefakte aus gemeldeten oder ausgenutzten Schwachstellen auf.

11.7 P26 – Richtlinie zur Lieferanten- und Drittparteiensicherheit. Koordiniert Offenlegungen, die Komponenten von Lieferanten betreffen.

11.8 P37 – Richtlinie zur rechtlichen und regulatorischen Compliance. Regelt Benachrichtigungen, Safe-Harbor-Formulierungen und Veröffentlichungen.

12. Referenzen

12.1 NIS2-Richtlinie (EU 2022/2555), Artikel 21 Absatz 2 Buchstabe e (Sicherheit in Entwicklung sowie Behandlung und Offenlegung von Schwachstellen)

12.2 Durchführungsverordnung (EU) 2024/2690 der Kommission, Anhang Abschnitt 6.10 (Technische Anforderungen an Prozesse zur Behandlung und Offenlegung von Schwachstellen)

12.3 ENISA Technical Guidance on Cybersecurity Risk Management Measures – Abschnitt zur Behandlung und Offenlegung von Schwachstellen

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (Maßnahme A.5.7 zu Bedrohungsinformationen und Offenlegung von Schwachstellen; Maßnahme A.8.28 zu sicherer Entwicklung)

12.5 ISO/IEC 29147:2018 (Leitlinien für die Offenlegung von Schwachstellen) und ISO/IEC 30111:2019 (Leitlinien für Prozesse zur Behandlung von Schwachstellen)