					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P30S					Dokumenttitel: **Richtlinie zur Reaktion auf Sicherheitsvorfälle (P30)**							
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	Klauseln 6.1, 6.3, 8	Vorfallmanagement, kontinuierliche Verbesserung, operative Steuerung
ISO/IEC 27002:2022	Maßnahmen 5.24, 5.25	Vorfallerkennung, Bereitschaft, Lernen aus Vorfällen
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Verfahren zur Behandlung von Informationssicherheitsvorfällen sowie deren Überwachung und Meldung
DSGVO	Artikel 33	Anforderungen an die Meldung von Datenschutzverletzungen
NIS2-Richtlinie	Artikel 23	Verpflichtende Meldung von Cybervorfällen
DORA	Artikel 17	Management von IKT-Vorfällen
COBIT 2019	DSS02, DSS04	Service- und Vorfallmanagement sowie Aufrechterhaltung des Geschäftsbetriebs

1. Zweck

1.1. Diese Richtlinie legt fest, wie die Organisation Informationssicherheitsvorfälle erkennt, meldet und auf diese reagiert, die ihre digitalen Systeme, Daten oder Dienste betreffen.

1.2. Sie dient dazu, Schäden zu minimieren, Kundendaten zu schützen und regulatorische Verpflichtungen wie die 72-Stunden-Meldepflicht der DSGVO bei Datenschutzverletzungen zu erfüllen.

1.3. Die Richtlinie stellt auch in kleinen Organisationen ohne dediziertes Sicherheitsteam klare Verantwortlichkeiten, Kommunikationswege und Nachverfolgungsmaßnahmen nach einem Vorfall sicher.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für:

2.1.1. alle Mitarbeitenden, Auftragnehmer und externen IT-Dienstleister

2.1.2. alle vom Unternehmen verwalteten Systeme und Dienste, einschließlich Websites, Cloud-Plattformen, mobiler Endgeräte, Laptops und E-Mail-Konten

2.1.3. alle Arten von Vorfällen, einschließlich:

2.1.3.1. unbefugtem Zugriff auf Daten oder Systeme

2.1.3.2. Schadsoftwareinfektionen oder Ransomware

2.1.3.3. Phishing- oder Social-Engineering-Versuchen

2.1.3.4. Systemausfällen infolge von Cyberangriffen oder Missbrauch

2.1.3.5. versehentlicher Offenlegung oder Löschung sensibler Informationen

2.1.3.6. Verlust oder Diebstahl geschäftlich genutzter Geräte oder Speichermedien

3. Ziele

3.1. Etablierung eines klaren Prozesses zur Erkennung und Eskalation von Sicherheitsvorfällen.

3.2. Sicherstellung, dass Vorfälle innerhalb vorab festgelegter Fristen gemeldet, protokolliert und bearbeitet werden.

3.3. Ermöglichung einer schnellen Schadensbegrenzung, Datenwiederherstellung und Wiederherstellung von Diensten.

3.4. Sicherstellung, dass betroffene Parteien, z. B. Kunden oder Aufsichtsbehörden, benachrichtigt werden, wenn dies gesetzlich erforderlich ist.

3.5. Verhinderung von Wiederholungen durch Ursachenanalyse, Korrekturmaßnahmen und Verbesserung der Richtlinie.

3.6. Unterstützung von KMU dabei, die Anforderungen für eine ISO-27001-Zertifizierung zu erfüllen und in Audits Rechenschaftsfähigkeit nachzuweisen.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführung (GM)

4.1.1. ist Eigentümerin dieser Richtlinie und stellt deren Umsetzung sicher.

4.1.2. überwacht die Maßnahmen zur Reaktion auf Sicherheitsvorfälle und genehmigt Meldungen an Aufsichtsbehörden oder Kunden.

4.1.3. prüft Berichte nach Vorfällen und stellt sicher, dass die Richtlinie bei Bedarf aktualisiert wird.

4.1.4. kann Koordinationsaufgaben delegieren, behält jedoch die Rechenschaftspflicht.

4.2. IT-Support-Dienstleister / Systemadministrator (intern oder extern)

4.2.1. erkennt und untersucht potenzielle Sicherheitsvorfälle.

4.2.2. setzt Eindämmungs- und Wiederherstellungsmaßnahmen um, z. B. die Sperrung von Zugängen oder die Wiederherstellung von Backups.

4.2.3. benachrichtigt die Geschäftsführung über alle bestätigten oder vermuteten Vorfälle innerhalb von 1 Stunde nach Entdeckung.

4.2.4. führt ein Vorfallprotokoll mit Zeitstempeln, Auswirkungsbewertung und Reaktionsmaßnahmen.

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

9. Anforderungen an Überprüfung und Aktualisierung

9.1. Regelmäßige Überprüfung

9.1.1. Diese Richtlinie muss mindestens alle 12 Monate durch die Geschäftsführung (GM) überprüft werden, um Folgendes sicherzustellen:

9.1.1.1. Ausrichtung an den Maßnahmen von ISO/IEC 27001:2022

9.1.1.2. Reaktionsfähigkeit auf neue Bedrohungen, Risiken und Vorfälle

9.1.1.3. fortlaufende Einhaltung rechtlicher und vertraglicher Verpflichtungen, z. B. DSGVO und DORA

9.2. Auslösende Ereignisse

9.2.1. Die Richtlinie muss außerdem nach Folgendem überprüft und aktualisiert werden:

9.2.1.1. jedem Vorfall mit hohem Schweregrad oder jeder Meldung an eine Aufsichtsbehörde

9.2.1.2. der Einführung neuer IT-Infrastruktur oder Systemänderungen

9.2.1.3. Änderungen rechtlicher Anforderungen in Bezug auf Sicherheitsverletzungen

9.3. Dokumentation der Überprüfung und Verteilung

9.3.1. Alle Überprüfungen und Änderungen müssen im Änderungsprotokoll der Richtlinie dokumentiert werden.

9.3.2. Aktualisierte Versionen müssen an alle Mitarbeitenden, Lieferanten und IT-Dienstleister verteilt werden, die an Sicherheits- oder Systembetriebsaufgaben beteiligt sind.

9.3.3. Nachweise der Sensibilisierung des Personals, z. B. Besprechungsnotizen oder E-Mail-Bestätigungen, müssen zur Auditbereitschaft aufbewahrt werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist in Abstimmung mit den folgenden SME-Richtlinien anzuwenden:

10.1.1. P1S – Informationssicherheitsrichtlinie: Legt die übergeordneten Erwartungen für die Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb fest, einschließlich des Umgangs mit Vorfällen.

10.1.2. P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt Befugnisse und Rechenschaftspflichten für Vorfallerkennung, Meldung und Eskalation fest.

10.1.3. P4S – Richtlinie zur Zugriffskontrolle: Ermöglicht den sofortigen Entzug von Zugriffsrechten während Maßnahmen zur Reaktion auf Sicherheitsvorfälle.

10.1.4. P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass alle Mitarbeitenden Sicherheitsvorfälle wirksam erkennen und melden können.

10.1.5. P17S – Richtlinie zu Datenschutz und Privatsphäre: Regelt die rechtmäßigen Verfahren zur Meldung von Datenschutzverletzungen nach DSGVO und unterstützt die Einhaltung regulatorischer Anforderungen bei Vorfällen.

10.1.6. P22S – Richtlinie zur Protokollierung und Überwachung: Stellt die erforderlichen Werkzeuge und die notwendige Transparenz für die Erkennung, Analyse und Auditierung von Sicherheitsereignissen bereit.

10.1.7. P31S – Richtlinie zur Beweissicherung und Forensik: Unterstützt die Untersuchung und regulatorische Belastbarkeit vorfallsbezogener Maßnahmen durch Vorgaben zum ordnungsgemäßen Umgang mit Beweismitteln.

10.2. Diese Richtlinien bilden gemeinsam den operativen Rahmen des KMU zur Erkennung von, Reaktion auf und Wiederherstellung nach Informationssicherheitsvorfällen.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 6.1 – Verlangt die Planung der Risikobehandlung einschließlich der Vorbereitung auf Vorfälle.

11.1.2. Klausel 6.3 – Unterstützt die kontinuierliche Verbesserung durch Erkenntnisse aus Sicherheitsereignissen.

11.1.3. Klausel 8.1 – Betont die operative Steuerung zur Handhabung von Vorfällen und Störungen.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 5.24 – Verlangt einen strukturierten Ansatz zur Meldung, Bewertung und Behandlung von Informationssicherheitsvorfällen.

11.2.2. Maßnahme 5.25 – Fokussiert auf das Lernen aus Vorfällen zur Verbesserung der zukünftigen Bereitschaft und der Resilienz von Systemen.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definiert Verfahren zum Umgang mit Informationssicherheitsvorfällen einschließlich Eindämmung und Wiederherstellung.

11.3.2. IR-5 – Legt Anforderungen an die Überwachung und Analyse von Vorfällen fest.

11.3.3. IR-6 – Schreibt Protokolle für die externe und interne Vorfallmeldung vor.

11.4. DSGVO

11.4.1. Artikel 33 – Verlangt die Meldung von Datenschutzverletzungen mit Angaben zu Umfang und Minderung an Aufsichtsbehörden innerhalb von 72 Stunden.

11.5. NIS2-Richtlinie (2022/2555)

11.5.1. Artikel 23 – Verlangt von wesentlichen und wichtigen Einrichtungen die Meldung erheblicher Vorfälle an zuständige Behörden unter Verwendung standardisierter Meldeformate.

11.6. DORA-Verordnung (2022/2554)

11.6.1. Artikel 17 – Verlangt von Finanzunternehmen die Klassifizierung, Meldung und Nachverfolgung IKT-bezogener Vorfälle und Störungen.

11.7. COBIT 2019

11.7.1. DSS02 – Serviceanfragen und Vorfälle verwalten: Gibt Leitlinien für den wirksamen Umgang mit betrieblichen Vorfällen und Sicherheitsvorfällen im Einklang mit den Governance-Zielen vor.

11.7.2. DSS04 – Kontinuität verwalten: Verknüpft die Reaktion auf Sicherheitsvorfälle mit umfassenderen Strategien zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung.