					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P30					Dokumenttitel: **Richtlinie zur Reaktion auf Sicherheitsvorfälle**							
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/Verordnung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8.1, Klausel 9	Strukturierte Prozesse für Risikomanagement und Reaktion auf Sicherheitsvorfälle
ISO/IEC 27002:2022	Maßnahmen 5.25–5.27	Rollen, Meldung, Reaktion und Verbesserung bei Sicherheitsvorfällen
NIST SP 800-53 Rev.5	IR-1 bis IR-9	Umfassender Lebenszyklus der Reaktion auf Sicherheitsvorfälle
EU-DSGVO	Artikel 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Fristen für die Meldung von Datenschutzverletzungen, Berichterstattung und Kommunikation mit betroffenen Personen
EU NIS2	Artikel 23(1)–(4)	Meldung an nationale Behörden und strukturierte Berichterstattung
EU DORA	Artikel 17(1)–(3)	Meldung schwerwiegender IKT-bezogener Vorfälle für Finanzunternehmen
COBIT 2019	DSS02, DSS04, MEA	Definiert, überwacht und beurteilt Vorfallmanagement, Aufrechterhaltung des Geschäftsbetriebs und Evaluierung

1. Zweck

1.1 Diese Richtlinie legt einen verbindlichen Rahmen für die Identifizierung, Meldung, Analyse, Eindämmung, Reaktion, Wiederherstellung und Nachbereitung von Informationssicherheitsvorfällen fest, die die Organisation betreffen.

1.2 Sie stellt sicher, dass Reaktionen rechtzeitig, koordiniert und wirksam erfolgen, um Betriebsunterbrechungen, finanzielle Verluste, Reputationsschäden und Verstöße gegen regulatorische Anforderungen zu minimieren.

1.3 Die Richtlinie unterstützt zudem die kontinuierliche Verbesserung der Cyber-Resilienz der Organisation durch Lessons Learned sowie die Überführung von Erkenntnissen aus Vorfällen in Governance, Werkzeuge und Schulungsprogramme.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 sämtliches Personal, einschließlich Mitarbeitender, Auftragnehmer, Berater und externer Dienstleister

2.1.2 alle Informationssysteme, Anwendungen, Infrastrukturen, Netzwerke und Daten – unabhängig davon, ob sie lokal, in der Cloud oder in hybriden Umgebungen betrieben werden

2.1.3 alle Arten von Sicherheitsvorfällen, einschließlich, aber nicht beschränkt auf:

2.1.3.1 unbefugten Zugriff oder Rechteausweitung

2.1.3.2 Schadsoftware- und Ransomware-Angriffe

2.1.3.3 Denial-of-Service-(DoS/DDoS)-Angriffe

2.1.3.4 Datenverlust, Datenabfluss oder Datenexfiltration

2.1.3.5 Insider-Missbrauch oder Richtlinienverstöße

2.1.3.6 Verletzungen der physischen Sicherheit mit Auswirkungen auf digitale Werte

2.2 Der Geltungsbereich dieser Richtlinie umfasst Erkennung, Triage, Untersuchung, Eskalation, Eindämmung, Umgang mit Nachweisen, Benachrichtigung, Wiederherstellung und Ursachenanalyse.

3. Ziele

3.1 Einrichtung einer wiederholbaren und skalierbaren Fähigkeit zur Reaktion auf Sicherheitsvorfälle, die eine schnelle Erkennung, Klassifizierung und Eindämmung von Sicherheitsvorfällen ermöglicht.

3.2 Minimierung der geschäftlichen Auswirkungen von Sicherheitsereignissen durch strukturierte Verfahren zur Eindämmung, Beseitigung und Systemwiederherstellung.

3.3 Sicherstellung, dass Meldung und Reaktion bei Vorfällen mit gesetzlichen, regulatorischen und vertraglichen Anforderungen übereinstimmen, insbesondere im Hinblick auf Fristen zur Meldung von Datenschutzverletzungen und den Umgang mit Nachweisen.

3.4 Unterstützung von Transparenz und Rechenschaftspflicht durch ordnungsgemäße Protokollierung, Dokumentation und Nachverfolgung von Kennzahlen für alle Sicherheitsvorfälle.

3.5 Förderung der kontinuierlichen Verbesserung durch Nachbetrachtungen von Vorfällen, Korrekturmaßnahmen und Schulungen für relevante Interessengruppen.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Verantwortet das Rahmenwerk für die Reaktion auf Sicherheitsvorfälle, stellt die Durchsetzung dieser Richtlinie sicher und überwacht die organisationsweite Koordination von Vorfällen.

4.1.2 Fungiert bei schwerwiegenden Vorfällen als primärer Ansprechpartner für Aufsichtsbehörden, Führungskräfte und die Rechtsabteilung.

4.2 Koordinator für die Reaktion auf Sicherheitsvorfälle

4.2.1 Koordiniert funktionsübergreifende Reaktionsteams, steuert Arbeitsabläufe und verfolgt den Status von Eindämmung und Wiederherstellung nach.

4.2.2 Veranlasst und leitet Prüfungen nach der Implementierung (PIR) und stellt sicher, dass Korrekturmaßnahmen protokolliert und umgesetzt werden.

[... 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 Diese Richtlinie muss mindestens jährlich überprüft und bei Bedarf überarbeitet werden, um Folgendes zu berücksichtigen:

9.1.1 Änderungen in der Bedrohungslage, bei Vorfallarten oder Angriffsvektoren

9.1.2 Lessons Learned aus schwerwiegenden Vorfällen, Beinahe-Vorfällen oder regulatorischen Feststellungen

9.1.3 Aktualisierungen einschlägiger Gesetze und Vorschriften (z. B. DSGVO, DORA, NIS2)

9.1.4 Rückmeldungen aus Übungen zur Reaktion auf Sicherheitsvorfälle und Nachbereitungen von Vorfällen

9.2 Der CISO ist für die Einleitung und Koordination des Überprüfungsprozesses verantwortlich, in Abstimmung mit:

9.2.1.1 Rechtsabteilung und DSB

9.2.1.2 SOC und IT-Betrieb

9.2.1.3 Teams für die Aufrechterhaltung des Geschäftsbetriebs und das Risikomanagement

9.2.1.4 Führungskräften

9.3 Änderungen an der Richtlinie müssen:

9.3.1 in einem versionskontrollierten Repository dokumentiert werden

9.3.2 allen betroffenen Teams mitgeteilt und in der Sensibilisierungsschulung aktualisiert werden

9.3.3 innerhalb von drei Monaten nach Genehmigung durch Tabletop- oder Live-Übungen zur Reaktion auf Sicherheitsvorfälle validiert werden

9.4 Dringende Aktualisierungen, die durch neu auftretende Bedrohungen, Audit-Feststellungen oder neu erlassene rechtliche Verpflichtungen ausgelöst werden, müssen unverzüglich umgesetzt und in der Änderungshistorie der Richtlinie vermerkt werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird durch die folgenden organisatorischen Richtlinien unterstützt und steht in Abhängigkeit zu ihnen:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt die übergeordnete Anforderung an risikobasierte und vorfallsbereite Betriebsabläufe fest.

10.1.2 P5 – Richtlinie zum Änderungsmanagement: Stellt sicher, dass Aktivitäten zur Eindämmung und Wiederherstellung, die Infrastruktur oder Services betreffen, formalen Verfahren folgen.

10.1.3 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Unterstützt die Schweregradklassifizierung von Vorfällen auf Basis der Datensensitivität.

10.1.4 P15 – Richtlinie für Backup und Wiederherstellung: Ermöglicht die Wiederherstellung nach Ransomware oder destruktiven Angriffen unter Sicherstellung der Integrität.

10.1.5 P18 – Richtlinie zu kryptografischen Kontrollen: Definiert Verschlüsselungsmaßnahmen zur Reduzierung der Auswirkungen von Vorfällen und der Risiken einer Datenexposition.

10.1.6 P22 – Richtlinie zur Protokollierung und Überwachung: Stellt die grundlegende Transparenz von Ereignissen, Alarmierung und Log-Aufbewahrung bereit, die für wirksame Erkennung und Forensik erforderlich sind.

10.1.7 P29 – Richtlinie zu Testdaten und Testumgebungen: Stellt sicher, dass Vorfälle mit Auswirkungen auf Nicht-Produktivumgebungen ebenfalls strukturiert und sicher behandelt werden.

10.1.8 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Validiert Vorfallsbereitschaft und Wirksamkeit der Reaktion auf Sicherheitsvorfälle durch strukturierte Audits und Compliance-Bewertungen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001: Klausel 8.1 – Operative Planung und Steuerung: Strukturierte Prozesse zur Steuerung von Risiken und zur Planung der Reaktion auf Sicherheitsvorfälle.

11.2 ISO/IEC 27002:2022 – Maßnahmen 5.25–5.27: Verantwortlichkeiten für Vorfallmanagement, Meldung, Reaktion, Kommunikation und Verbesserung.

11.3 NIST SP 800-53 Rev.5: IR-1 bis IR-9, AU-6, PL-2: Umfassende Anforderungen an den Lebenszyklus der Reaktion auf Sicherheitsvorfälle, Audit und Sicherheitsplanung.

11.4 EU-DSGVO: Artikel 33/34: Meldepflichten gegenüber Aufsichtsbehörden sowie Anforderungen an die Benachrichtigung betroffener Personen (mit festgelegten Ausnahmen).

11.5 EU-NIS2-Richtlinie (2022/2555): Artikel 23: Verpflichtende nationale Meldung mit Zwischen- und Abschlussberichten.

11.6 EU DORA (2022/2554): Artikel 17: Anforderungen an die Meldung von IKT-Vorfällen an Behörden für Finanzinstitute.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Management von Servicevorfällen und Aufrechterhaltung des Geschäftsbetriebs sowie Überwachung von Leistung und Konformität.