					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P31					Dokumenttitel: **Richtlinie zur Beweissicherung und IT-Forensik**							
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/Regulierung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	
ISO/IEC 27002:2022	Maßnahmen 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Teile 1 und 3	
NIST SP 800-53 Rev. 5	IR-1 bis IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Forensik mobiler Geräte und Datenträger	Mobile- und Datenträgerforensik
NIST SP 800-86	Integration forensischer Techniken	Integration forensischer Techniken in die Incident Response
DSGVO	Artikel 5, 33–34	
EU NIS2	Artikel 23(1)–(4)	
EU DORA	Artikel 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Zweck

1.1 Diese Richtlinie legt einen strukturierten und rechtlich belastbaren Rahmen für die Identifizierung, Erhebung, Sicherung, Analyse und Entsorgung digitaler Beweismittel bei tatsächlichen oder vermuteten Sicherheitsvorfällen fest.

1.2 Sie stellt sicher, dass Prozesse zur forensischen Bereitschaft und zum Umgang mit Beweismitteln:

1.2.1 die Integrität der Beweismittel und die Chain of Custody wahren,

1.2.2 interne Untersuchungen, Gerichtsverfahren oder regulatorische Meldungen unterstützen,

1.2.3 an international anerkannten forensischen Standards und Anforderungen an die rechtliche Zulässigkeit ausgerichtet sind.

1.3 Die Richtlinie unterstützt die Verpflichtung der Organisation zu proaktiver Incident Response, rechtlicher und regulatorischer Compliance sowie Transparenz in der Governance und minimiert zugleich operative Beeinträchtigungen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeitenden, Auftragnehmer, Lieferanten und Dienstleister, die mit Systemadministration, der Behandlung von Informationssicherheitsvorfällen oder Untersuchungstätigkeiten befasst sind,

2.1.2 alle Endgeräte, Server, Anwendungen, Netzwerke und Cloud-Plattformen, die der organisatorischen Kontrolle oder vertraglichen Verantwortung unterliegen,

2.1.3 jeden Vorfall oder jedes Ereignis, das den Umgang mit Beweismitteln erfordert, einschließlich:

2.1.3.1 Insider-Bedrohungen, Datenschutzverletzungen oder Betrugsuntersuchungen,

2.1.3.2 missbräuchlicher Nutzung von Systemen oder Zugangsdaten,

2.1.3.3 Vorfällen im Bereich Operational Technology (OT) oder industrieller Steuerungssysteme,

2.1.3.4 Verstößen beim physischen Zugriff mit Bezug zu digitalen Assets.

2.2 Die Richtlinie regelt außerdem jede Interaktion mit externen forensischen Dienstleistern oder Strafverfolgungsbehörden im Rahmen rechtlicher und regulatorischer Eskalationen oder Verfahren.

3. Ziele

3.1 Sicherstellung einer schnellen, sicheren und richtlinienkonformen Erhebung von Beweismitteln bei Sicherheitsereignissen oder Untersuchungen.

3.2 Wahrung der Integrität, Authentizität und Zulässigkeit erhobener digitaler Beweismittel durch strikte Kontrolle von Zugriff, Protokollierung und Prüfverfahren.

3.3 Sicherstellung, dass alle forensischen Tätigkeiten mit rechtlichen und regulatorischen Verpflichtungen abgestimmt sind, einschließlich Datenschutz, Arbeitsrecht und Beschränkungen internationaler Übermittlungen.

3.4 Unterstützung der Nachbereitung von Vorfällen, der Ursachenanalyse und der Verbesserung von Kontrollen durch hochwertige forensische Ergebnisse.

3.5 Integration der forensischen Bereitschaft in das Informationssicherheitsmanagementsystem (ISMS) zur Unterstützung von Audits, Meldungen von Datenschutzverletzungen und Entscheidungen der Geschäftsleitung.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 ist Eigentümer dieser Richtlinie und stellt sicher, dass alle forensischen Tätigkeiten rechtlich belastbar, auditierbar und risikobasiert sind.

4.1.2 genehmigt die Eskalation an externe Rechtsinstanzen und forensische Dienstleister.

4.2 Forensische Analysten / Incident-Handler

4.2.1 verantworten die Erhebung, Sicherung und technische Analyse von Beweismitteln.

4.2.2 stellen sicher, dass die Chain of Custody ordnungsgemäß dokumentiert und aufrechterhalten wird.

4.2.3 dokumentieren alle im Rahmen der Untersuchungen eingesetzten Maßnahmen, Feststellungen und Werkzeugeinstellungen.

[... 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 aktualisiert werden, um Folgendes abzubilden:

9.1.1 Änderungen von Gesetzen, Vorschriften oder Rechtsprechung, die forensische Verfahren oder Datenverarbeitung betreffen,

9.1.2 Aktualisierungen branchenweit anerkannter forensischer Standards oder Werkzeugsätze,

9.1.3 Erkenntnisse aus Reviews nach Vorfällen, Rechtsstreitigkeiten oder Audit-Feststellungen,

9.1.4 technologische Änderungen an Plattformen, Geräten oder Systemen, die Gegenstand von Untersuchungen sind.

9.2 Für den Überprüfungsprozess ist der CISO verantwortlich; er muss Konsultationen mit folgenden Stellen einschließen:

9.2.1 Rechtsabteilung und Compliance,

9.2.2 Datenschutzbeauftragter (DPO),

9.2.3 Security Operations und Forensik,

9.2.4 Interne Revision und Compliance-Funktion.

9.3 Alle Änderungen müssen:

9.3.1 versionskontrolliert und im Richtlinien-Repository gespeichert werden,

9.3.2 an betroffene Interessenträger, einschließlich Forensik- und Response-Teams, kommuniziert werden,

9.3.3 von Aktualisierungen einschlägiger Betriebsverfahren und Schulungsunterlagen begleitet werden.

9.4 Außerplanmäßige Überprüfungen müssen nach jedem kritischen Vorfall ausgelöst werden, der mit unsachgemäßem Umgang mit Beweismitteln, dem Versagen der Chain of Custody oder Problemen der rechtlichen Zulässigkeit verbunden ist.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist mit den folgenden organisatorischen Richtlinien abgestimmt und wird durch diese unterstützt:

10.1.1 P1 – Informationssicherheitsrichtlinie: legt das grundlegende Mandat für Untersuchungen, Beweismittelkontrolle und die Einhaltung anwendbarer Gesetze fest.

10.1.2 P5 – Änderungsmanagement-Richtlinie: stellt sicher, dass Systeme, die Gegenstand einer Untersuchung sind, während laufender forensischer Prozesse nicht verändert werden.

10.1.3 P14 – Richtlinie zur Datenaufbewahrung und Entsorgung: regelt die sichere Entsorgung und die Aufbewahrungsfristen für Beweismittel und fallbezogene Daten.

10.1.4 P18 – Richtlinie zu kryptografischen Kontrollen: legt Anforderungen an die Verschlüsselung für die Speicherung und Übermittlung sensibler oder beweisrelevanter Daten fest.

10.1.5 P22 – Richtlinie zur Protokollierung und Überwachung: stellt die Verfügbarkeit von Ereignisprotokollen und Telemetriedaten für die Beweiserhebung und forensische Korrelation sicher.

10.1.6 P30 – Incident-Response-Richtlinie: definiert die Triage von Sicherheitsvorfällen und Eskalationswege, in denen forensische Verfahren ausgelöst werden.

10.1.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung: validiert die Einhaltung forensischer Protokolle und der Anforderungen an die Chain of Custody durch regelmäßige Audits.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an internationalen Standards für Forensik und Incident Handling ausgerichtet und stellt die Integrität von Beweismitteln, rechtliche Belastbarkeit und Compliance über mehrere Rechtsordnungen hinweg sicher.

11.2 ISO/IEC 27001

11.2.1 Klausel 8.1 – unterstützt die operative Steuerung der forensischen Bereitschaft und von Beweismittelverfahren.

11.3 ISO/IEC 27002

11.3.1 Anhang A, Maßnahme 5.25 – Verantwortlichkeiten für das Vorfallmanagement: fordert definierte Rollen für den Umgang mit Informationssicherheitsvorfällen und Untersuchungen.

11.3.2 Anhang A, Maßnahme 5.26 – Meldung von Informationssicherheitsereignissen: unterstützt die Erhebung ereignisbezogener Artefakte als Beweismittel.

11.3.3 Anhang A, Maßnahme 5.27 – Reaktion auf Informationssicherheitsvorfälle: verlangt eine strukturierte, beweismittelgestützte Behebung und Untersuchung.

11.3.4 Anhang A, Maßnahme 8.27 – sichere Entwicklung und Forensik (soweit anwendbar): behandelt den Schutz von Systemen und Werkzeugen während Untersuchungen.

11.4 ISO/IEC 27035:2016 (Teile 1 und 3)

11.4.1 beschreibt die Grundsätze der Vorfallserkennung, Reaktion und forensischen Bereitschaft, einschließlich Planung, Chain of Custody und Management von Vorfallsbeweismitteln.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 bis IR-9, AU-6, PL-2: definiert strukturierte Anforderungen für Planung, Erkennung, Analyse, Eindämmung und Reaktion auf Sicherheitsvorfälle. Unterstützt die Erhebung und Auditierbarkeit von Beweismitteln (AU-6) und stellt die Abstimmung mit Sicherheits- und Datenschutzplänen für Systeme (PL-2) während forensischer Untersuchungen sicher.

11.6 NIST SP 800-86

11.6.1 gibt Leitlinien für die Integration forensischer Prozesse in den erweiterten Incident-Response-Lebenszyklus und zur Sicherstellung der forensischen Bereitschaft.

11.7 NIST SP 800-101 Rev. 1

11.7.1 konzentriert sich auf Best Practices zur Erhebung, Sicherung und Analyse digitaler Medien und Beweismittel aus mobilen Geräten in rechtlich belastbarer Weise.

11.8 DSGVO (2016/679)

11.8.1 Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten: gilt für Beweismittel, die personenbezogene oder sensible Daten enthalten, und stellt Datenminimierung und Zweckbindung sicher.

11.8.2 Artikel 33–34 – Meldung von Datenschutzverletzungen: Forensische Daten unterstützen die Einhaltung von Meldepflichten bei Datenschutzverletzungen und rechtlichen Offenlegungsprozessen.

11.9 EU NIS2-Richtlinie (2022/2555)

11.9.1 Artikel 23 – Meldepflichten: Forensische Dokumentation und Feststellungen unterstützen rechtzeitige und zutreffende Vorfallmeldungen an zuständige Behörden.

11.10 EU DORA (2022/2554)

11.10.1 Artikel 17 – Meldung von IKT-Vorfällen: verlangt detaillierte Ursachenanalysen und beweisbezogene Aufzeichnungen zu wesentlichen IKT-bezogenen Vorfällen, insbesondere im Finanzsektor.

11.11 COBIT 2019

11.11.1 DSS01.07 – Sicherheitsvorfälle verwalten: verlangt Vorfallsdokumentation und sorgfältige Untersuchungen.

11.11.2 DSS05.04 – Sicherheitsuntersuchungen verwalten: betont die Sicherung digitaler Beweismittel und die Unterstützung disziplinarischer und rechtlicher Maßnahmen.