					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P31S					Dokumenttitel: **Richtlinie zur Beweissicherung und 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 Normen und regulatorischen Anforderungen

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.1, 6.3, 8	Risikobasierte Planung, Verbesserungsmaßnahmen und operative Kontrollen zur Sicherstellung der Integrität von Beweismitteln
ISO/IEC 27002:2022	Maßnahmen 5.24–5.27	Leitet die sichere Handhabung, Nachbereitung von Vorfällen und evidenzbasierte Verbesserungen an
ISO/IEC 27035-3:2016	Klauseln 6.3, 6.4, 7	Stellt eine ordnungsgemäße Planung, rechtmäßige Erhebung und sichere Handhabung digitaler Beweismittel mit Dokumentation der Beweismittelkette sicher
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Forensische Bereitschaft, Schutz von Audit-Logs und wirksame Integration in die Reaktion auf Informationssicherheitsvorfälle
EU GDPR	Artikel 33, 34	Dokumentation und Nachvollziehbarkeit bei Datenschutzverletzungen mit personenbezogenen Daten
EU NIS2	Artikel 23	Nachvollziehbare Vorfallmeldung und sichere Handhabung von Beweismitteln
EU DORA	Artikel 17(1), 17(2)	Stellt die Erhebung, Speicherung und Aufbewahrung von Beweismitteln für IKT-bezogene Vorfälle, forensische Belastbarkeit und Anfragen von Aufsichtsbehörden sicher
COBIT 2019	DSS05.06, DSS05.07	Verlässliche Protokollierung und strukturierte Handhabung von Beweismitteln für sichere, auditierbare Untersuchungen

1. Zweck

1.1. Diese Richtlinie legt fest, wie die Organisation digitale Beweismittel im Zusammenhang mit Sicherheitsvorfällen, Datenschutzverletzungen oder internen Untersuchungen handhabt. Sie stellt sicher, dass Beweismittel rechtssicher und auditbereit erhoben, gespeichert und aufbewahrt werden und sowohl interne Entscheidungen als auch mögliche externe Maßnahmen unterstützen.

1.2. Die Richtlinie ermöglicht es kleinen Organisationen, die Integrität von Protokollen, Dateien und Systemabbildern zu schützen und zugleich die gebotene Sorgfalt nach ISO/IEC 27001, DSGVO und zugehörigen Standards nachzuweisen.

1.3. Sie unterstützt die forensische Bereitschaft, ohne fortgeschrittene technische Ressourcen oder ein Vollzeit-IT-Team vorauszusetzen, indem sie klare Verantwortlichkeiten, Prozesse und Aufbewahrungsanforderungen festlegt.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für:

2.1.1. alle Mitarbeitenden, IT-Dienstleister und externen Berater, die an der Reaktion auf Vorfälle, Untersuchungen oder der Analyse von Verstößen beteiligt sind

2.1.2. alle Unternehmenssysteme, einschließlich Laptops, mobiler Geräte, Server, E-Mail-Konten, SaaS-Plattformen und Cloud-Speicher (z. B. Microsoft 365, Google Workspace)

2.1.3. jedes Ereignis, das Beweismittel für interne disziplinarische Maßnahmen, Rechtsverteidigung, Versicherungsansprüche oder den Austausch mit Aufsichtsbehörden erfordert

2.2. Dies umfasst sowohl tatsächliche als auch vermutete Ereignisse in Bezug auf:

2.2.1. Datenabfluss

2.2.2. Insider-Bedrohungen oder Missbrauch

2.2.3. Sicherheitsvorfälle (z. B. Schadsoftware, unbefugter Zugriff)

2.2.4. Kundenbeschwerden, die eine digitale Validierung erfordern

2.2.5. Anfragen von Aufsichtsbehörden oder Strafverfolgungsbehörden

3. Ziele

3.1. Es ist sicherzustellen, dass alle Beweismittel so erhoben und gehandhabt werden, dass ihre Integrität, Authentizität und Beweismittelkette gewahrt bleiben.

3.2. Eine versehentliche Änderung, Löschung oder unsachgemäße Handhabung von Protokollen, Dateien oder Systemabbildern, die für Untersuchungen erforderlich sein können, ist zu verhindern.

3.3. Ein einheitlicher, auditierbarer Ansatz für die Handhabung von Beweismitteln ist bereitzustellen, der rechtliche und regulatorische Anforderungen erfüllt (z. B. Meldung von Datenschutzverletzungen nach DSGVO, Nachvollziehbarkeit nach NIS2).

3.4. Klare Rollen und Verantwortlichkeiten sind festzulegen, um eine schnelle, sichere und rechtlich konforme Sicherung von Beweismitteln bei Sicherheitsvorfällen zu gewährleisten.

3.5. Die Richtlinie unterstützt die forensische Bereitschaft auf KMU-Niveau bei gleichzeitiger Begrenzung der Komplexität und ohne unnötige Beeinträchtigung des Tagesgeschäfts.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführung (GM)

4.1.1. Genehmigt alle formellen Untersuchungen, die eine Beweissicherung erfordern.

4.1.2. Prüft und genehmigt Vorfallsberichte, die potenzielle rechtliche oder disziplinarische Maßnahmen betreffen.

4.1.3. Entscheidet, ob externe Rechtsberater oder Aufsichtsbehörden benachrichtigt werden müssen.

4.1.4. Stellt sicher, dass diese Richtlinie regelmäßig überprüft und aktualisiert wird.

4.2. IT-Dienstleister / Systemadministrator

4.2.1. Erhebt und sichert digitale Beweismittel gemäß festgelegten sicheren Verfahren.

4.2.2. Dokumentiert Zeitstempel, Systemdetails und Bearbeitungsschritte.

4.2.3. Sichert alle erhobenen Materialien an einem geschützten Speicherort.

4.2.4. Unterstützt bei Bedarf die forensische Analyse.

[... 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. Jährliche Richtlinienüberprüfung

9.1.1. Diese Richtlinie ist mindestens einmal alle 12 Monate durch die Geschäftsführung (GM) zu überprüfen, um Folgendes zu bestätigen:

9.1.1.1. Einhaltung der Maßnahmen aus Anhang A der ISO/IEC 27001

9.1.1.2. fortbestehende Relevanz für aktuelle digitale Plattformen und IT-Services

9.1.1.3. Angemessenheit der Verfahren für Protokollierung, Aufbewahrung von Beweismitteln und forensische Bereitschaft

9.2. Auslösende Ereignisse für eine Richtlinienüberarbeitung

9.2.1. Die Richtlinie ist außerdem nach folgenden Ereignissen zu überprüfen und zu aktualisieren:

9.2.1.1. jedem wesentlichen Vorfall, der eine Beweissicherung erfordert

9.2.1.2. einem nicht bestandenen Audit oder einer regulatorischen Anfrage, bei der die Integrität von Beweismitteln infrage gestellt wurde

9.2.1.3. der Einführung neuer Werkzeuge oder Verfahren für die Reaktion auf Informationssicherheitsvorfälle oder das Systemmonitoring

9.2.1.4. rechtlichen Änderungen (z. B. aktualisierte Leitlinien zur DSGVO oder NIS2)

9.3. Änderungsgenehmigung und Verteilung

9.3.1. Alle Änderungen müssen durch die Geschäftsführung geprüft und genehmigt werden.

9.3.2. Die aktualisierte Version ist bereitzustellen für:

9.3.2.1. IT-Dienstleister und Berater, die an Untersuchungen beteiligt sind

9.3.2.2. alle Mitarbeitenden mit Aufgaben in der Systemadministration

9.3.3. Eine aktualisierte Kopie ist im Richtlinienarchiv des Unternehmens aufzubewahren und Auditoren auf Anfrage bereitzustellen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie steht in wechselseitiger Abhängigkeit zu den folgenden auf KMU ausgerichteten Richtlinien:

10.1.1. P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt Befugnisse für Vorfallsuntersuchungen, Entscheidungen zu Beweismitteln und rechtliche Eskalationen fest.

10.1.2. P4S – Richtlinie zur Zugriffskontrolle: Stellt sicher, dass während Untersuchungen nur autorisiertes Personal auf sensible Systeme und Protokolle zugreifen kann.

10.1.3. P22S – Richtlinie zur Protokollierung und Überwachung: Stellt die Rohdaten bereit, die als forensische Beweismittel verwendet werden, und legt Anforderungen an Aufbewahrung, Zugriffskontrolle und Protokollierung fest.

10.1.4. P30S – Richtlinie zur Reaktion auf Informationssicherheitsvorfälle: Löst die Notwendigkeit der Beweissicherung aus und definiert den operativen Ablauf bis zur forensischen Sicherung.

10.1.5. P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass als Beweismittel erhobene personenbezogene Daten gemäß DSGVO und verwandten Vorschriften rechtmäßig verarbeitet werden.

10.2. Diese Richtlinien wirken zusammen, um Rechtsbeständigkeit, die Integrität von Untersuchungen und vollständige Auditbereitschaft nach ISO/IEC 27001:2022 zu unterstützen.

11. Referenznormen und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 6.1 – Die risikobasierte Planung umfasst die Bereitschaft für Reaktionsmaßnahmen und Verfahren für Beweismittel.

11.1.2. Klausel 6.3 – Unterstützt Verbesserungsmaßnahmen auf Grundlage von Beweismitteln aus Vorfällen.

11.1.3. Klausel 8.1 – Verlangt operative Kontrollen zur Sicherstellung der Integrität von Beweismitteln.

11.2. ISO/IEC 27002

11.2.1. Maßnahmen 5.24–5.27 – Leiten die sichere Handhabung, Nachbereitung von Vorfällen und evidenzbasierte Verbesserungen an.

11.3. ISO/IEC 27035-3

11.3.1. Klauseln 6.3, 6.4 und 7.3 stellen eine ordnungsgemäße Planung, rechtmäßige Erhebung und sichere Handhabung digitaler Beweismittel während der Reaktion auf Vorfälle sicher, einschließlich Aufbewahrung und Dokumentation der Beweismittelkette.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 und AU-12 stellen forensische Bereitschaft, den Schutz von Audit-Logs und die wirksame Integration der Beweissicherung in den Lebenszyklus der Reaktion auf Informationssicherheitsvorfälle sicher.

11.5. NIST SP 800-86

11.5.1. Definiert Best Practices für die Sicherung, Analyse und den Schutz digitaler Beweismittel im Rahmen der Reaktion auf Vorfälle.

11.6. EU GDPR

11.6.1. Artikel 33–34 – Verlangen Dokumentation und Nachvollziehbarkeit von Vorfällen und Beweismitteln bei der Meldung von Datenschutzverletzungen mit personenbezogenen Daten.

11.7. EU NIS2-Richtlinie (2022/2555)

11.7.1. Artikel 23 – Verlangt nachvollziehbare Vorfallmeldung und sichere Handhabung von Beweismitteln für wesentliche und wichtige Einrichtungen.

11.8. EU DORA

11.8.1. Artikel 17(1) – Stellt sicher, dass Beweismittel im Zusammenhang mit IKT-bezogenen Vorfällen so erhoben und gespeichert werden, dass sie forensische Untersuchungen unterstützen.

11.8.2. Artikel 17(2) – Verlangt, dass Finanzunternehmen alle relevanten Daten und Protokolle im Zusammenhang mit Sicherheitsereignissen aufbewahren, ausgerichtet auf forensische Belastbarkeit und Anfragen von Aufsichtsbehörden.

11.9. COBIT 2019

11.9.1. DSS05.06 – Vorfälle überwachen, erkennen und melden: Hebt die Bedeutung verlässlicher Protokollierung zur Unterstützung von Untersuchungen hervor.

11.9.2. DSS05.07 – Vorfälle untersuchen und Maßnahmen ergreifen: Verlangt eine strukturierte Handhabung von Beweismitteln, um sichere und auditierbare Untersuchungen zu ermöglichen.