					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P03					Dokumenttitel: **Richtlinie zur zulässigen Nutzung**							
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 geltenden Standards und regulatorischen Anforderungen

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 5	Legt Verhaltensregeln und Anforderungen für die Richtlinie zur zulässigen Nutzung fest
ISO/IEC 27002:2022	Maßnahmen 6.1, 6.2, 8.1, 8.12	Gibt Leitlinien für Verantwortlichkeiten in der Informationssicherheit, Sensibilisierung sowie die Governance von Geräten und Daten vor
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Zugriffskontrollen sowie Kontrollen zur Sensibilisierung und zu Verhaltensregeln mit Relevanz für die Nutzung von IT-Assets
EU-DSGVO	Artikel 5(1)(f), 32; Erwägungsgrund 39	Schreibt Vertraulichkeit und Integrität vor, verlangt technische und organisatorische Maßnahmen sowie Rechtsgrundlagen für die ordnungsgemäße Nutzung
EU NIS2	Artikel 21(2)(a–d)	Verlangt operative Richtlinien und Schulungen zur sicheren Nutzung
EU DORA	Artikel 5	Unterstützt das IKT-Risikomanagement durch Regelungen zum Benutzerverhalten
COBIT 2019	APO07, BAI05, DSS05, MEA01	Personalmanagement, Änderungsmanagement, verwaltete Sicherheitsdienste sowie Überwachung von Compliance und Leistung

1. Zweck

1.1 Diese Richtlinie legt die zulässige und unzulässige Nutzung der Informationssysteme, IT-Ressourcen, Kommunikationsmittel und Datenverarbeitungspraktiken der Organisation fest.

1.2 Sie stellt sicher, dass alle Benutzer ihre Verantwortlichkeiten bei der Nutzung von IKT-Assets der Organisation verstehen und dass ihr Handeln die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) sowie die rechtmäßige Informationsverarbeitung unterstützt.

1.3 Die Richtlinie erfüllt ISO/IEC 27001:2022, Maßnahme 5.10, indem sie Verhaltensregeln für die Systemnutzung festlegt und technische sowie organisatorische Schutzmaßnahmen anwendet, um das Risiko von Fehlgebrauch, Fahrlässigkeit oder Missbrauch zu minimieren.

1.4 Sie unterstützt außerdem Untersuchungs- und Durchsetzungsmaßnahmen, einschließlich Incident Response sowie disziplinarischer Maßnahmen bei Verstößen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Personen und Einheiten, denen Zugriff auf die Informationssysteme und Assets der Organisation gewährt wurde, einschließlich, aber nicht beschränkt auf:

2.1.1 Mitarbeiter, Auftragnehmer, Berater, Praktikanten und Leiharbeitskräfte

2.1.2 externe Lieferanten mit Systemzugriff oder übertragenen administrativen Rollen

2.1.3 Gäste oder Partner, die von der Organisation bereitgestellte oder autorisierte IT-Infrastruktur nutzen

2.2 Der Geltungsbereich umfasst sämtliche Technologie- und Datenwerte der Organisation, einschließlich:

2.2.1 Arbeitsplatzrechner, Laptops, mobile Endgeräte und Server

2.2.2 Netzwerkinfrastruktur und cloudbasierte Dienste

2.2.3 E-Mail, Messaging, Dateispeicher, Kollaborationsplattformen und VPNs

2.2.4 Daten im Ruhezustand, bei der Übertragung oder in Verarbeitung, unabhängig von Format oder Speicherort

2.2.5 jedes persönliche Gerät, das im Rahmen einer Bring-Your-Own-Device-(BYOD)-Regelung mit den Systemen der Organisation verbunden wird

2.3 Diese Richtlinie ist in allen Arbeitsumgebungen verbindlich, einschließlich:

2.3.1 Unternehmensstandorten und Produktionsstandorten

2.3.2 Standorten für Remote-Arbeit oder hybride Arbeitsmodelle

2.3.3 Außeneinsatzumgebungen oder von Dritten betriebenen Räumlichkeiten

2.4 Alle Benutzer müssen diese Richtlinie als Voraussetzung für den Zugriff auf Unternehmenssysteme oder den Umgang mit Unternehmensdaten bestätigen und einhalten.

3. Ziele

3.1 Festlegung und Durchsetzung von Regeln für die autorisierte Nutzung von IT-Ressourcen.

3.2 Verhinderung von unbefugtem Zugriff, Datenabfluss oder Schäden infolge fahrlässiger oder böswilliger Nutzung.

3.3 Schutz von Unternehmensnetzwerken, Assets und Daten vor Bedrohungen, die durch Benutzerverhalten eingebracht werden.

3.4 Unterstützung gesetzlicher und vertraglicher Verpflichtungen durch den Nachweis der gebotenen Sorgfalt bei der Governance von IT-Ressourcen.

3.5 Sicherstellung von Konsistenz und Klarheit bei der Anwendung disziplinarischer Maßnahmen und von Prozessen für das Ausnahmemanagement.

3.6 Förderung einer Kultur der ethischen, sicheren und verantwortungsvollen Nutzung digitaler und physischer IT-Ressourcen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt die Richtlinie zur zulässigen Nutzung und stellt sicher, dass sie mit den Geschäftszielen, regulatorischen Anforderungen und den Werten der Organisation im Einklang steht.

4.1.2 Stellt Ressourcen für Durchsetzung, Schulung, Überwachung und Richtlinienüberprüfung bereit.

4.1.3 Überprüft im Rahmen der ISMS-Governance den Status der Compliance und disziplinarische Maßnahmen im Zusammenhang mit Richtlinienverstößen.

4.2 IT- und Informationssicherheitsteams

4.2.1 Setzen technische Schutzmaßnahmen zur Durchsetzung dieser Richtlinie um, darunter:

4.2.2 Inhaltsfilterung, Schutz vor Schadsoftware, Endgeräteschutz und Netzwerküberwachungswerkzeuge

4.2.3 E-Mail-Sicherheitskonfigurationen und Data Loss Prevention (DLP)-Lösungen

4.2.4 Sperrlisten und Positivlisten für Software, Hardware und Websites

4.2.5 Führen ein Verzeichnis zugelassener und verbotener Software, Geräte und Dienste.

4.2.6 Untersuchen vermutete Verstöße gegen die Richtlinie zur zulässigen Nutzung, sichern forensische Beweise und unterstützen gegebenenfalls disziplinarische oder rechtliche Maßnahmen.

4.2.7 Arbeiten mit Personalwesen und Rechtsabteilung bei Vorfallbearbeitung, Eskalation und Meldepflichten zusammen.

[... 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 Auslöser und Häufigkeit der Überprüfung

9.1.1 Diese Richtlinie ist zu überprüfen:

9.1.1.1 mindestens jährlich

9.1.1.2 nach wesentlichen Änderungen an Technologie oder Infrastruktur

9.1.1.3 nach Vorfällen oder Audit-Feststellungen, die Lücken in der Durchsetzung aufzeigen

9.1.1.4 als Reaktion auf Änderungen geltender Gesetze oder vertraglicher Anforderungen

9.2 Verantwortlichkeit und Genehmigung

9.2.1 Der CISO oder der benannte ISMS-Manager ist für den Überprüfungsprozess verantwortlich.

9.2.2 Aktualisierungen müssen durch die Geschäftsleitung genehmigt und organisationsweit kommuniziert werden.

9.2.3 Die Bestätigung aktualisierter Bestimmungen ist bei erneuter Veröffentlichung der Richtlinie erneut einzuholen.

9.3 Dokumentenmanagement

9.3.1 Die Richtlinie muss die folgenden Metadaten und Versionsangaben enthalten:

9.3.1.1 Titel, Kennung und Klassifizierungsstufe

9.3.1.2 Richtlinienverantwortlicher und Dokumentenverantwortlicher

9.3.1.3 Änderungshistorie und Begründung für Aktualisierungen

9.3.1.4 Überprüfungsdatum und nächstes geplantes Aktualisierungsdatum

9.3.1.5 Referenzen auf Verteilungs- und Bestätigungsprotokolle

9.3.2 Die Masterkopie ist versioniert im ISMS-Dokumentenrepository aufzubewahren.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist im Zusammenhang mit den folgenden Richtlinien auszulegen:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt grundlegende Verhaltenserwartungen und das Engagement der obersten Leitung für die zulässige Nutzung fest.

10.1.2 P4 – Zugriffssteuerungsrichtlinie: Definiert Berechtigungen und Rechte im Zusammenhang mit Benutzern, Systemen und Datenzugriff und setzt damit unmittelbar die Grenzen der zulässigen Nutzung.

10.1.3 P6 – Risikomanagement-Richtlinie: Behandelt verhaltensbezogene Risiken und unterstützt Überwachungs- und Behandlungsmaßnahmen im Zusammenhang mit benutzerbedingten Bedrohungen.

10.1.4 P7 – Richtlinie für Onboarding und Austritt: Stellt sicher, dass Bedingungen zur zulässigen Nutzung beim Eintritt bestätigt und beim Austritt widerrufen werden.

10.1.5 P9 – Richtlinie für Remote-Arbeit: Erweitert die Bestimmungen zur zulässigen Nutzung auf Remote- und hybride Arbeitsumgebungen.

10.2 Diese zugehörigen Richtlinien bilden ein mehrschichtiges Verteidigungsmodell für verhaltensbezogene, technische und vertragliche Governance.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie zur zulässigen Nutzung ist an international anerkannten Standards und rechtlichen Rahmenwerken ausgerichtet, um durchsetzbare, auditierbare und risikobasierte Verhaltenskontrollen für die gesamte Nutzung digitaler und physischer Informationssysteme sicherzustellen.

11.2 ISO/IEC 27001:2022

11.2.1 Maßnahme 5.10 – Zulässige Nutzung von Informationswerten und anderen zugehörigen Assets: Diese Richtlinie erfüllt unmittelbar die Anforderung, Regeln für die angemessene Nutzung von IT-Ressourcen festzulegen, zu kommunizieren und durchzusetzen.

11.2.2 Anhang A, Maßnahme 6.1 – Verantwortung für Informationssicherheit: Weist klare Verantwortlichkeiten für Benutzerverhalten und Aufsicht über die Compliance zu.

11.2.3 Anhang A, Maßnahme 6.2 – Sensibilisierung, Schulung und Training zur Informationssicherheit: Integrierte Schulungen und Prozesse zur Richtlinienbestätigung sind Bestandteil der Durchsetzung der Richtlinie zur zulässigen Nutzung.

11.2.4 Anhang A, Maßnahme 8.1 – Endgeräte von Benutzern und 8.12 – Data Loss Prevention (DLP): Behandelt zulässiges Verhalten auf Benutzergeräten und regelt Aktivitäten, die zu Datenexposition oder Datenabfluss führen könnten.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Zugriffskontrolle für mobile Geräte) und AC-20 (Nutzung externer Informationssysteme): Diese Richtlinie definiert Benutzerpflichten und Beschränkungen für Bring-Your-Own-Device (BYOD) und den Zugriff auf Systeme Dritter.

11.3.2 PL-4 (Verhaltensregeln): Stellt detaillierte Anforderungen an die zulässige Nutzung bereit, die mit dieser Richtlinie im Einklang stehen.

11.3.3 AT-2 (Schulung zur Sensibilisierung für Informationssicherheit): Wird durch Benutzerschulungen und dokumentierte Richtlinienbestätigung unterstützt.

11.3.4 AU-2 (Audit-Ereignisse) und AU-12 (Audit-Erzeugung): Die Durchsetzung stützt sich auf die Überwachung von Benutzerhandlungen und die Alarmierung bei Verstößen.

11.4 EU-DSGVO (2016/679):

11.4.1 Artikel 5(1)(f): Schreibt die Sicherheit und Integrität personenbezogener Daten vor; diese Richtlinie mindert Risiken, die durch menschliches Verhalten und unbefugte Nutzung entstehen.

11.4.2 Artikel 32: Verlangt technische und organisatorische Maßnahmen wie Verhaltenskontrollen und Nutzungsbeschränkungen zum Schutz personenbezogener Daten.

11.4.3 Erwägungsgrund 39: Hebt hervor, dass nur erforderlicher Zugriff und eine rechtmäßige Nutzung von Daten durch autorisierte Personen sichergestellt werden dürfen.

11.5 EU-NIS2-Richtlinie (2022/2555):

11.5.1 Artikel 21(2)(a–d): Verlangt operative Richtlinien und Schulungen für die sichere Systemnutzung, die diese Richtlinie zur zulässigen Nutzung durch die Festlegung von Verhalten, Überwachung und Durchsetzungsprozessen bereitstellt.

11.6 EU-DORA (2022/2554):

11.6.1 Artikel 5: Diese Richtlinie unterstützt das IKT-Risikomanagementrahmenwerk, indem sie Regeln für die Mensch-System-Interaktion festlegt und die Exposition gegenüber verhaltensbasierten Cyberrisiken minimiert.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Setzt Benutzerverantwortlichkeiten und Sensibilisierung über den gesamten Beschäftigungslebenszyklus hinweg durch.

11.7.2 BAI05 – Managed Organizational Change: Verankert die Governance zur zulässigen Nutzung in Änderungsprozessen, die sich auf das Benutzerverhalten auswirken.

11.7.3 DSS05 – Managed Security Services: Unterstützt die Überwachung von Benutzeraktivitäten, verhaltensbezogene Warnmeldungen und automatisierte Reaktionsmechanismen.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: Die Richtlinie definiert Kennzahlen und Mechanismen zur Validierung der Einhaltung von Verhaltenserwartungen durch Benutzer.