					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P04					Dokumenttitel: **Richtlinie zur Zugriffskontrolle**							
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/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.15, 5.17, 5.18	Verwaltung des logischen und physischen Zugriffs
ISO/IEC 27002:2022	Maßnahmen 8.2, 8.3	Rollenbasierter Zugriff und Identitätsmanagement
NIST SP 800-53 Rev. 5	AC-1 bis AC-20, IA-1 bis IA-8	Kontrollen für Konten- und Zugriffsverwaltung, Identitätsauthentifizierung
EU-DSGVO	Artikel 5 Abs. 1 Buchst. f, 32 Abs. 1 Buchst. b; Erwägungsgrund 39	Datenschutz und Datenminimierung
EU-NIS2	Artikel 21 Abs. 2 Buchst. c–e	Zugriffs- und Benutzerauthentifizierung sowie Schutz von Assets
EU-DORA	Artikel 6, 9 Abs. 2	IKT- und Benutzerzugriff sowie starke Kontrollen für Drittparteien
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Onboarding, Betrieb, Überwachung, Compliance

1. Zweck

1.1 Diese Richtlinie legt verbindliche Grundsätze, Verantwortlichkeiten und Kontrollanforderungen für die Verwaltung des Zugriffs auf Informationssysteme, Anwendungen, physische Einrichtungen und Datenbestände in der gesamten Organisation fest.

1.2 Sie stellt sicher, dass Zugriffe auf Grundlage des Geschäftsbedarfs, der Aufgabenfunktion und des Risikoprofils gewährt werden und dass Grundsätze wie das Prinzip der minimalen Berechtigung, Need-to-know und Funktionstrennung durchgesetzt werden.

1.3 Die Richtlinie unterstützt die Umsetzung von ISO/IEC 27001:2022, Klausel 5.15, sowie zugehöriger Kontrollen für logischen und physischen Zugriff, Benutzerauthentifizierung und das Management des Zugriffslebenszyklus.

1.4 Diese Richtlinie dient dem Schutz digitaler und physischer Ressourcen vor unbefugter Nutzung, Missbrauch und Kompromittierung.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Benutzer, Systeme und Einrichtungen innerhalb des ISMS-Geltungsbereichs, einschließlich:

2.1.1 Mitarbeiter, Auftragnehmer, Lieferanten sowie temporär eingesetztes Personal

2.1.2 Lokale Infrastruktur, Cloud-basierte Systeme und hybride Umgebungen

2.1.3 Alle Unternehmens-IKT-Assets – Hardware, Software, Daten und gesicherte physische Bereiche

2.1.4 Logischer Zugriff (z. B. Systeme, Netzwerke, Anwendungen, APIs) und physischer Zugriff (z. B. Gebäude, Rechenzentren)

2.2 Sie regelt den Zugriff über den gesamten Lebenszyklus von Identitäten und deren Interaktion mit Ressourcen hinweg, vom Onboarding und der Bereitstellung bis zu Rollenänderungen und Offboarding.

2.3 Die Richtlinie umfasst auch Bring-Your-Own-Device-(BYOD)- und Fernzugriffsszenarien und stellt sicher, dass Kontrollen standort- und eigentumsmodellübergreifend konsistent angewendet werden.

3. Ziele

3.1 Umsetzung sicherer, rollenbasierter Zugriffskontrollen zur Unterstützung der betrieblichen Integrität und der Einhaltung regulatorischer Anforderungen.

3.2 Sicherstellung, dass Zugriffsrechte angemessen genehmigt, überwacht und fristgerecht entzogen werden.

3.3 Verhinderung unbefugter Zugriffe, der Eskalation von Berechtigungen und des Fortbestands veralteter Zugriffsrechte.

3.4 Unterstützung von Zero-Trust-Grundsätzen durch die standardmäßige Verweigerung von Zugriffen, sofern diese nicht ausdrücklich genehmigt und begründet sind.

3.5 Bereitstellung belastbarer Nachweise für Auditoren und Interessenträger durch nachweisgestützte, automatisierte Zugriffsüberprüfungen und die Durchsetzung dieser Richtlinie.

3.6 Verankerung der Zugriffskontrolle in Geschäftsprozessen, HR-Ereignissen im Beschäftigungslebenszyklus und technischen Architekturen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt die Richtlinie zur Zugriffskontrolle und stellt ein angemessenes Budget sowie ausreichende personelle Ressourcen für ihre Durchsetzung sicher.

4.1.2 Bewertet Zugriffskontrollrisiken im Rahmen von Managementbewertungen und weist Rechenschaftspflichten auf strategischer Ebene zu.

4.2 CISO / ISMS-Manager

4.2.1 Ist für das Rahmenwerk der Zugriffskontrolle verantwortlich und stellt die Ausrichtung an ISO/IEC 27001 und verwandten Standards sicher.

4.2.2 Koordiniert die Durchsetzung der Richtlinie, Kontrolltests und die Berichterstattung zu Kennzahlen der Zugriffskontrolle.

4.2.3 Beaufsichtigt risikobasierte Zugriffsmodelle und überwacht systemische Kontrolllücken.

[... 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 muss überprüft werden:

9.1.1.1 Jährlich oder

9.1.1.2 Nach einer wesentlichen Änderung der IT-Infrastruktur, regulatorischer Anforderungen oder des Risikoprofils

9.1.1.3 Nach Vorfällen, die Schwächen in den Zugriffskontrollen aufdecken

9.1.1.4 Bei wesentlichen Änderungen von Authentifizierungstechnologien oder Identitätsplattformen

9.2 Zuständigkeit und Verfahren der Überprüfung

9.2.1 Der CISO oder der benannte ISMS-Verantwortliche steuert den Überprüfungszyklus unter Einbeziehung von:

9.2.1.1 Feststellungen aus internen Audits

9.2.1.2 Ergebnissen und Kennzahlen aus Zugriffsüberprüfungen

9.2.1.3 Rechtlichen und regulatorischen Aktualisierungen

9.2.1.4 Änderungen an Technologieplattformen

9.2.2 Alle Überarbeitungen müssen durch die Geschäftsleitung genehmigt und allen Interessenträgern kommuniziert werden.

9.2.3 Betroffene Benutzer können verpflichtet werden, die Richtlinie nach wesentlichen Aktualisierungen erneut zu bestätigen.

9.3 Versionskontrolle und Dokumentation

9.3.1 Die Master-Version ist mit folgenden Metadaten im ISMS-Dokumentenrepository zu speichern:

9.3.1.1 Versionsnummer und Änderungsprotokoll

9.3.1.2 Datum des Inkrafttretens und Datum der nächsten Überprüfung

9.3.1.3 Verantwortlicher und Genehmigungsbefugnis

9.3.1.4 Verteilungs- und Bestätigungsnachweise

9.3.2 Ersetzte Versionen müssen archiviert und für mindestens 3 Jahre zugänglich gehalten werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist funktional abhängig von den nachfolgenden Richtlinien und gemeinsam mit ihnen auszulegen:

10.1.1 P01 – Informationssicherheitsrichtlinie: Definiert das Sicherheitsbekenntnis der Organisation und die übergeordneten Erwartungen an die Zugriffskontrolle.

10.1.2 P03 – Richtlinie zur zulässigen Nutzung: Legt verhaltensbezogene Bedingungen für den Zugriff und die Rechenschaftspflicht der Benutzer für die verantwortungsvolle Systemnutzung fest.

10.1.3 P05 – Richtlinie zum Änderungsmanagement: Regelt, wie Änderungen an Zugriffskonfigurationen, Rollen oder Gruppenstrukturen sicher umgesetzt und getestet werden müssen.

10.1.4 P07 – Richtlinie für Onboarding und Austritt: Steuert die Einrichtung und den Entzug von Zugriffsrechten im Einklang mit Ereignissen des Benutzerlebenszyklus.

10.1.5 P11 – Richtlinie zur Verwaltung von Benutzerkonten und Berechtigungen: Operationalisiert kontobezogene Kontrollen und ergänzt diese Richtlinie um Leitlinien zur technischen Durchsetzung von Zugriffskontrollen.

10.2 Zusammen bilden diese Richtlinien ein kohärentes und durchsetzbares Rahmenwerk für die Zugriffsgovernance über Geschäftsbereiche und Technologien hinweg.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:2022:

11.1.1 Klausel 5.15 – Zugriffskontrolle: Diese Richtlinie erfüllt die Anforderung, den Zugriff auf Informationen und andere zugehörige Assets auf Grundlage von Geschäfts- und Informationssicherheitsanforderungen zu kontrollieren.

11.1.2 Klausel 5.17 – Identitätsmanagement und Klausel 5.18 – Authentifizierungsinformationen: Diese Anforderungen werden durch Identitätsbereitstellung, Authentifizierungsmechanismen und Berechtigungszuweisungen operationalisiert.

11.1.3 Anhang-A-Maßnahmen 8.2 (Zugriffskontrolle) und 8.3 (Identitätsmanagement): Bilden die Grundlage für die Kontrollziele dieser Richtlinie, einschließlich rollenbasiertem Zugriff, Integration des Benutzerlebenszyklus und Schutz privilegierter Zugriffe.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 AC-Familie (AC-1 bis AC-20): Diese Richtlinie unterstützt die NIST-Anforderungen an die Zugriffskontrolle für physische und logische Systeme, einschließlich Richtliniendefinition (AC-1), Kontenverwaltung (AC-2) und Funktionstrennung (AC-5).

11.2.2 IA-Familie (IA-1 bis IA-8): Bietet Leitlinien für Identitätsauthentifizierung, Schutz von Zugangsdaten und MFA.

11.2.3 AU-2, AU-12: Die nach dieser Richtlinie durchgesetzten Anforderungen an Protokollierung und Auditierung unterstützen die Rechenschaftspflicht der Benutzer und die Untersuchung von Vorfällen.

11.2.4 PE-2 bis PE-6: Betreffen physische Zugriffsbeschränkungen, die durch diese Richtlinie teilweise mittels Ausweiskontrollen und Berechtigungen für den Gebäudezugang durchgesetzt werden.

11.3 EU-DSGVO (2016/679):

11.3.1 Artikel 5 Abs. 1 Buchst. f: Personenbezogene Daten müssen vor unbefugtem Zugriff geschützt werden. Diese Richtlinie stellt die technische und prozessuale Durchsetzung dieses Grundsatzes sicher.

11.3.2 Artikel 32 Abs. 1 Buchst. b: Verlangt die Implementierung von Zugriffskontrollen, Pseudonymisierung und Verschlüsselung zur Verhinderung einer unbefugten Verarbeitung personenbezogener Daten.

11.3.3 Erwägungsgrund 39: Verlangt die Minimierung des Zugriffs auf personenbezogene Daten; dies wird hier durch das Prinzip der minimalen Berechtigung und Anforderungen an die Begründung des Zugriffs durchgesetzt.

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

11.4.1 Artikel 21 Abs. 2 Buchst. c–e: Diese Richtlinie ermöglicht technische und organisatorische Maßnahmen zur Zugriffskontrolle, Benutzerauthentifizierung und zum Schutz von Assets bei wesentlichen und wichtigen Einrichtungen.

11.5 EU-DORA (2022/2554):

11.5.1 Artikel 6: Verlangt IKT-Risikomanagementrichtlinien, die ausdrücklich die Benutzerzugriffsverwaltung und Kontrollen des Identitätslebenszyklus umfassen. Diese Richtlinie erfüllt diese Anforderung für den Finanz- und IKT-Dienstleistungssektor.

11.5.2 Artikel 9 Abs. 2: Diese Richtlinie unterstützt die Durchsetzung starker Zugriffskontrollen als Teil des Managements von IKT-Dienstleistungen durch Drittparteien und innerhalb von Konzernstrukturen.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: Unterstützt die Zugriffsgovernance durch Onboarding- und Offboarding-Kontrollen.

11.6.2 BAI03 – Managed Solutions Identification and Build: Verankert Anforderungen an die Zugriffskontrolle in Systemdesign- und Änderungsprozessen.

11.6.3 DSS01 – Managed Operations und DSS05 – Sicherheitsdienste verwalten: Regeln die Durchsetzung logischer Zugriffsbeschränkungen und die Überwachung von Verstößen.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Unterstützt Audit- und Assurance-Mechanismen zur Validierung der Wirksamkeit von Zugriffskontrollen.