					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P11S					Dokumenttitel: **Richtlinie zur Verwaltung von Benutzerkonten und Berechtigungen**							
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**

An Standards und regulatorischen Anforderungen ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.3, 8	Rollen, Verantwortlichkeiten sowie operative Planung und Steuerung für die Verwaltung von Benutzerzugriffen
ISO/IEC 27002:2022	Maßnahme 8	Maßnahmen zur Vergabe, Überprüfung und Entziehung erhöhter Berechtigungen
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Kontoerstellung, Überwachung, Prinzip der minimalen Berechtigung und Funktionstrennung
EU NIS2	Artikel 21(2)(d)	Verwaltung von Benutzerzugriffen für wesentliche und wichtige Einrichtungen
EU DORA	Artikel 9(2)(b)	Kontrolle privilegierter Zugriffe in Finanzunternehmen
COBIT 2019	DSS05.03, DSS05.04	Bereitstellung, Entzug von Zugriffsrechten und regelmäßige Überprüfung von Benutzerzugriffen
DSGVO	Artikel 32	Angemessene Zugriffskontrollen zum Schutz personenbezogener Daten

1. Zweck

1.1 Diese Richtlinie legt verbindliche Regeln für die sichere, konsistente und nachvollziehbare Verwaltung von Benutzerkonten und Zugriffsrechten fest. Sie stellt sicher, dass nur autorisierte Benutzer Zugriff auf Systeme und Daten erhalten und dass dieser Zugriff ihrer Rolle und ihren Verantwortlichkeiten angemessen ist.

1.2 Ein wirksames Management von Konten und Berechtigungen ist wesentlich, um unbefugte Zugriffe zu verhindern, Insider-Bedrohungen zu minimieren und die Einhaltung von ISO/IEC 27001, der DSGVO und weiteren regulatorischen Anforderungen sicherzustellen.

1.3 Diese Richtlinie ermöglicht der Organisation, Verantwortlichkeiten und Zuständigkeiten für die Nutzung von Konten festzulegen, Rechteerweiterungen zu überwachen und zu auditieren sowie Zugriffe sicher zu deaktivieren oder zu entziehen, sobald sie nicht mehr benötigt werden.

1.4 Sie schützt zudem den Geschäftsbetrieb vor Bedienfehlern oder Missbrauch infolge übermäßiger oder unzureichend überwachter Zugriffe und trägt dazu bei, das Risiko versehentlichen Datenabflusses, des Missbrauchs von Berechtigungen oder der Nichteinhaltung regulatorischer Anforderungen zu verringern.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeiter, Praktikanten, Auftragnehmer und Benutzer Dritter mit Zugriff auf die IT-Systeme der Organisation

2.1.2 alle Systeme, Geräte, Dienste und Plattformen, die von der Organisation oder in ihrem Auftrag verwaltet werden, einschließlich Cloud-Plattformen, lokaler Infrastruktur und Tools von Drittanbietern

2.2 Sie umfasst alle Arten von Benutzerkonten, einschließlich:

2.2.1 personenbezogener Benutzerkonten (z. B. E-Mail-Konten, Systemanmeldungen)

2.2.2 Administratorkonten und Konten auf Systemebene

2.2.3 temporärer Zugangsdaten, Gastzugänge oder Zugangsdaten für Dritte

2.2.4 Dienstkonten, die von Anwendungen oder Automatisierungssystemen verwendet werden

2.3 Die Richtlinie gilt für den gesamten Lebenszyklus von Konten – von der Erstellung und Genehmigung bis zur Änderung, Überwachung und Deaktivierung. Dies umfasst die initiale Bereitstellung im Rahmen des Onboardings, Zugriffsüberprüfungen bei Rollenänderungen sowie den Entzug von Zugriffsrechten im Rahmen des Offboardings.

3. Ziele

3.1 Allen Systembenutzern sind eindeutige und nachvollziehbare Benutzeridentitäten zuzuweisen, um Rechenschaftspflicht sicherzustellen und die Nutzung gemeinsam genutzter Zugangsdaten auszuschließen.

3.2 Das Prinzip der minimalen Berechtigung ist durchzusetzen, sodass Benutzern nur der zur Erfüllung ihrer Aufgaben erforderliche Mindestzugriff gewährt wird.

3.3 Unbefugter Zugriff auf sensible Systeme oder Daten ist durch klar dokumentierte Genehmigungs- und Überprüfungsprozesse zu verhindern.

3.4 Benutzerkonten sind unverzüglich zu deaktivieren, wenn sie nicht mehr erforderlich sind, z. B. bei Austritt, Vertragsende oder Rollenänderungen.

3.5 Durch die Dokumentation sämtlicher Kontoänderungen, Genehmigungen und regelmäßiger Überprüfungen ist eine sichere und auditierbare Umgebung aufrechtzuerhalten.

3.6 Rechteerweiterungen sind streng zu kontrollieren, unabhängig zu genehmigen und zu protokollieren; erhöhte Berechtigungen sind unverzüglich zu entziehen, sobald sie nicht mehr benötigt werden.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 Trägt die Gesamtverantwortung für die Durchsetzung dieser Richtlinie.

4.1.2 Stellt sicher, dass die Verfahren zur Kontenverwaltung mit den Anforderungen der ISO/IEC-27001-Zertifizierung und den einschlägigen rechtlichen Verpflichtungen (z. B. DSGVO) im Einklang stehen.

4.1.3 Ist über jeden unbefugten Zugriff, Informationssicherheitsvorfall oder Richtlinienverstoß im Zusammenhang mit Benutzerkonten unverzüglich zu informieren.

4.1.4 Überwacht Richtlinienüberprüfungen, Audits und Durchsetzungsmaßnahmen.

4.2 IT-Leitung oder externer IT-Dienstleister

4.2.1 Ist für die technische Umsetzung der Konten- und Berechtigungskontrollen in allen von der Organisation genutzten Systemen verantwortlich.

4.2.2 Darf Benutzerkonten ausschließlich auf Grundlage dokumentierter Genehmigungen bereitstellen, ändern und deaktivieren.

4.2.3 Muss Passwortkomplexität, Bildschirmsperre bei Inaktivität, Multi-Faktor-Authentifizierung (sofern verfügbar) und Systemprotokollierung durchsetzen.

4.2.4 Muss sichere Aufzeichnungen über sämtliche Zugriffsgenehmigungen, die Kontoinhaberschaft, Rechteerweiterungen und den Entzug von Zugriffsrechten führen.

4.2.5 Hat unbefugte oder verwaiste Benutzerkonten zu überwachen und Abweichungen dem GM zu melden.

[... 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 ist mindestens jährlich durch den GM und die IT-Leitung zu überprüfen, um die Einhaltung der folgenden Anforderungen sicherzustellen:

9.1.1 aktuelle Maßnahmen und Leitlinien nach ISO/IEC 27001:2022

9.1.2 regulatorische Aktualisierungen (z. B. DSGVO, DORA, NIS2)

9.1.3 Änderungen an Systemen, Diensten oder der Geschäftsstruktur

9.2 Überprüfungen sind außerdem durchzuführen nach:

9.2.1 wesentlichen Informationssicherheitsvorfällen oder Auditfeststellungen

9.2.2 größeren Änderungen an IT-Systemen oder der Kontenarchitektur

9.2.3 Einführung neuer Plattformen, die eine Integration in die Zugriffskontrolle erfordern

9.3 Sämtliche Änderungen müssen durch den GM genehmigt und den betroffenen Mitarbeitern klar kommuniziert werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt Rechenschaftspflicht und Entscheidungsbefugnisse für Zugriffsgenehmigungen und Aufsicht fest.

10.2 P4S – Richtlinie zur Zugriffskontrolle: Regelt die systemweite Durchsetzung der Zugriffskontrolle und Authentifizierungsverfahren.

10.3 P7S – Richtlinie für Onboarding und Austritt: Stellt sicher, dass Kontoerstellung und Kontenentzug in durch den Personalbereich gesteuerte Personaländerungen eingebunden sind.

10.4 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Schult Benutzer in sicheren Kontenpraktiken und Nutzungsvorgaben.

10.5 P30S – Richtlinie für die Reaktion auf Sicherheitsvorfälle: Definiert die zu ergreifenden Maßnahmen, wenn der Missbrauch von Konten zu einer Sicherheitsverletzung oder unbefugten Offenlegung führt.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 5.3: Verlangt, dass Rollen und Verantwortlichkeiten für die Informationssicherheit klar zugewiesen und durchgesetzt werden.

11.1.2 Klausel 8.1: Die operative Planung und Steuerung muss die Verwaltung von Benutzerzugriffen umfassen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.2: Beschreibt technische und prozessuale Maßnahmen zur Vergabe, Überprüfung und Entziehung erhöhter Berechtigungen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Verlangt die Erstellung, Überwachung und den Entzug von Konten auf Grundlage definierter Rollen und Prozesse.

11.3.2 AC-5: Behandelt die Funktionstrennung zur Verhinderung von Interessenkonflikten oder Missbrauch von Berechtigungen.

11.3.3 AC-6: Verlangt die Anwendung des Prinzips der minimalen Berechtigung auf sämtliche Zugriffsrechte.

11.4 DSGVO

11.4.1 Artikel 32: Verlangt angemessene Zugriffskontrollen zum Schutz personenbezogener Daten vor unbefugtem Zugriff oder unbefugter Veränderung.

11.5 EU NIS2

11.5.1 Artikel 21(2)(d): Verlangt die Verwaltung von Benutzerzugriffen als Bestandteil zentraler Sicherheitsmaßnahmen für wesentliche und wichtige Einrichtungen.

11.6 EU DORA

11.6.1 Artikel 9(2)(b): Verlangt von Finanzunternehmen die Implementierung von Zugriffskontrollen zur Beschränkung und Überwachung privilegierter Rechte.

11.7 COBIT 2019

11.7.1 DSS05.03: Legt die Bereitstellung und den Entzug von Zugriffsrechten als Teil der IT-Governance fest.

11.7.2 DSS05.04: Fordert die fortlaufende Überprüfung und Ausrichtung von Benutzerzugriffen an organisatorischen Rollen.