					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P04S					Dokumenttitel: **Zugriffsrichtlinie**							
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**

Abgleich mit Standards und regulatorischen Anforderungen

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 5	
ISO/IEC 27002:2022	Maßnahmen 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 bis AC-5	
EU-DSGVO	Artikel 32	
EU NIS2	Artikel 21(2)(b)	
EU DORA	Artikel 9	
COBIT 2019	APO07, DSS01	

1. Zweck

1.1. Diese Richtlinie legt fest, wie die Organisation den Zugriff auf Systeme, Daten und Einrichtungen verwaltet, um sicherzustellen, dass nur autorisierte Personen entsprechend den geschäftlichen Erfordernissen auf Informationen zugreifen können.

1.2. Sie definiert klare Vorgaben für die Bereitstellung, Änderung, Überwachung und Entziehung von Benutzerzugriffen, um das Risiko unbefugter Zugriffe zu minimieren und die Einhaltung geltender Gesetze und Standards zu unterstützen.

1.3. Die Richtlinie setzt das Least-Privilege-Prinzip durch und verlangt, dass Zugriffe auf das für die Ausübung der jeweiligen Tätigkeit erforderliche Mindestmaß beschränkt werden.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Personen, die Zugriffe auf die IT-Systeme, Netzwerke, Daten oder Einrichtungen der Organisation nutzen oder verwalten, einschließlich:

2.1.1. Mitarbeitende

2.1.2. Auftragnehmer

2.1.3. Zeitarbeitskräfte

2.1.4. Externe IT-Dienstleister

2.2. Sie umfasst den Zugriff auf:

2.2.1. Unternehmensanwendungen, Dateifreigaben und Datenbanken

2.2.2. E-Mail-, VPN- und Fernzugriffssysteme

2.2.3. Cloud-Dienste, die für geschäftliche Zwecke genutzt werden

2.2.4. Physischen Zutritt zu geschützten Bereichen, wie Büros oder Serverräumen

2.3. Diese Richtlinie ist für alle Geräte, Plattformen und Standorte verbindlich, einschließlich vom Unternehmen bereitgestellter Geräte sowie genehmigter Bring Your Own Device (BYOD).

3. Ziele

3.1. Sicherstellen, dass Zugriffsrechte nur nach formaler Genehmigung auf Grundlage der Rolle und einer geschäftlichen Begründung vergeben werden.

3.2. Unbefugten oder übermäßigen Zugriff auf sensible Daten, Systeme oder Infrastrukturen verhindern.

3.3. Eindeutige Verfahren für die Bereitstellung, Änderung und Entziehung von Benutzerzugriffen festlegen.

3.4. Regelmäßige Zugriffsüberprüfungen sowie eine automatisierte oder manuelle Protokollierung zur Unterstützung von Audits vorschreiben.

3.5. Die technische Durchsetzung von Zugriffsbeschränkungen durch Konfiguration und Überwachung sicherstellen.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführer

4.1.1. Genehmigt diese Richtlinie und stellt sicher, dass ausreichende Ressourcen für die Umsetzung wirksamer Zugriffskontrollen zur Verfügung stehen.

4.1.2. Genehmigt Ausnahmen und überprüft die jährlichen Zugriffsaudits.

4.2. IT-Manager / externer IT-Support-Dienstleister

4.2.1. Verantwortet die Bereitstellung, Änderung und Entziehung von Benutzerkonten.

4.2.2. Führt ein Zugriffskontrollregister mit sämtlichen Aktivitäten (Anlage, Änderung, Entziehung).

4.2.3. Implementiert rollenbasierte Zugriffskontrollen (RBAC) und setzt starke Authentifizierung durch (z. B. Multi-Faktor-Authentifizierung).

4.2.4. Überprüft Zugriffsprotokolle auf verdächtige Aktivitäten und meldet Auffälligkeiten an den Geschäftsführer.

[... 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 Überprüfung der Richtlinie

9.1.1. Der IT-Manager muss diese Richtlinie jährlich überprüfen. Änderungen im rechtlichen, technischen oder organisatorischen Kontext müssen eine unverzügliche Aktualisierung auslösen.

9.2. Auslöser für Überprüfungen

9.2.1. Die Richtlinie muss außerdem überprüft werden, wenn eines der folgenden Ereignisse eintritt:

9.2.2. Wesentliche Systemänderungen oder Cloud-Migrationen

9.2.3. Änderungen von Rollen oder der Organisationsstruktur

9.2.4. Ein Sicherheitsvorfall mit unbefugtem Zugriff

9.2.5. Regulatorische Änderungen (z. B. Aktualisierungen der DSGVO, NIS2 oder DORA)

9.3. Dokumentation und Kommunikation von Änderungen

9.3.1. Überarbeitungen müssen mit Versionshistorie dokumentiert, vom Geschäftsführer genehmigt und an sämtliches betroffenes Personal kommuniziert werden.

9.4. Verfügbarkeit und Schulung

9.4.1. Diese Richtlinie muss allen Mitarbeitenden zur Verfügung gestellt werden; relevante Schulungen müssen im Rahmen des Onboardings und danach jährlich erfolgen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist in Abstimmung mit den folgenden SME-Richtlinien anzuwenden, um die durchgängige Umsetzung sicherer Zugriffspraktiken sicherzustellen:

10.1.1. P3S – Richtlinie zur zulässigen Nutzung: Stellt sicher, dass Benutzer die zulässigen Verhaltensweisen bei gewährtem Zugriff verstehen.

10.1.2. P5S – Änderungsmanagement-Richtlinie: Stellt sicher, dass Zugriffsrechte mit genehmigten Systemänderungen abgestimmt sind.

10.1.3. P7S – Richtlinie für Onboarding und Austritt: Definiert auslösende Ereignisse für die Bereitstellung und den Entzug von Zugriffsberechtigungen.

10.1.4. P17S – Datenschutz- und Privatsphäre-Richtlinie: Stellt sicher, dass Zugriffskontrollen mit Schutzmaßnahmen für personenbezogene Daten abgestimmt sind.

10.1.5. P30S – Richtlinie für Incident Response (P30): Definiert, wie zugriffsbezogene Vorfälle (z. B. Missbrauch oder Datenschutzverletzungen) behandelt und untersucht werden.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Maßnahme 5.15 – Verlangt formalisierte Richtlinien und Prozesse zur Zugriffskontrolle.

11.2. ISO/IEC 27002

11.2.1. Maßnahmen 5.15–5.17 – Enthalten detaillierte Vorgaben zum rollenbasierten Zugriff, zur Benutzerzugriffsverwaltung und zum Umgang mit privilegierten Zugängen.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 bis AC-5 – Verlangen strukturierte Richtlinien für das Zugriffsmanagement, einschließlich Kontoberechtigungen, Überprüfung und Überwachung.

11.4. EU-DSGVO

11.4.1. Artikel 32 – Verlangt technische und organisatorische Maßnahmen (wie Zugriffsmanagement), um Datensicherheit und Vertraulichkeit sicherzustellen.

11.5. EU-NIS2-Richtlinie

11.5.1. Artikel 21(2)(b) – Schreibt operative Maßnahmen für Zugriffskontrolle und Identitätsmanagement vor, um unbefugten Systemzugriff zu verhindern.

11.6. EU DORA

11.6.1. Artikel 9 – Betont die sichere Steuerung von IKT-Risiken, einschließlich robuster Zugriffskontrollen für Finanzunternehmen.

11.7. COBIT 2019

11.7.1. APO07 Personalmanagement – Fordert definierte und durchgesetzte Verantwortlichkeiten für Zugriffe.

11.7.2. DSS01 – Betriebsmanagement: Umfasst Verfahren zur Verwaltung des logischen Zugriffs und zur Aufrechterhaltung sicherer Betriebsumgebungen.