					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P07S					Dokumenttitel: **Richtlinie für Onboarding und Offboarding**							
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 Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.2, 7	Anforderungen an die Personalsicherheit und Sensibilisierung
ISO/IEC 27002:2022	Maßnahmen 6.2, 6.5	Sicherheitspraktiken für Onboarding und Offboarding
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Beendigung von Beschäftigungsverhältnissen; Lebenszyklus von Benutzerkonten; Planung
EU NIS2	Artikel 21(2)(h)	Personalsicherheit und Zugriffslebenszyklus
EU DORA	Artikel 12	Zugriffskontrollen und Entzug von Zugriffsrechten für IKT-Systeme
COBIT 2019	APO07, DSS01	Personalsicherheit, Kontrollen für logischen und physischen Zugriff
EU DSGVO	Artikel 32	Sicherheit personenbezogener Daten während des Beschäftigungsverhältnisses

1. Zweck

1.1 Diese Richtlinie definiert den Prozess für das Onboarding neuer Mitarbeitender oder Auftragnehmer sowie für den sicheren Entzug von Zugriffsberechtigungen, wenn Personen ausscheiden oder ihre Rolle wechseln.

1.2 Sie stellt sicher, dass Zugriffe nach dem Prinzip der geringsten Privilegien vergeben werden, alle Vermögenswerte erfasst sind und kritische Maßnahmen wie die Deaktivierung von Systemzugängen und die Wiederherstellung von Daten zeitnah abgeschlossen werden.

1.3 Diese Richtlinie unterstützt die Einhaltung regulatorischer Anforderungen, die operative Integrität und den Datenschutz durch strukturierte und auditierbare Onboarding- und Offboarding-Aktivitäten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle festangestellten und befristet beschäftigten Mitarbeitenden

2.1.2 Auftragnehmer, Berater und Praktikanten

2.1.3 externe Dienstleister mit Systemzugriff oder physischem Zutritt

2.2 Sie umfasst:

2.2.1 Onboarding: Einrichtung von Benutzerkonten, Gewährung von Zugriffsberechtigungen, Ausgabe von Geräten

2.2.2 Offboarding: Entzug von Zugriffsberechtigungen, Rückgabe von Unternehmenswerten und sicherer Abschluss digitaler Identitäten

2.2.3 interne Rollenänderungen, die eine Neukonfiguration von Zugriffsberechtigungen oder eine Neuzuweisung von Vermögenswerten erfordern

2.3 Sie gilt für alle Geräte, Plattformen und Standorte, die für offizielle Geschäftszwecke genutzt werden.

3. Ziele

3.1 Sicherstellen, dass neue Beschäftigte Zugriff und Ressourcen auf Grundlage verifizierter Rollen und Verantwortlichkeiten erhalten.

3.2 Sicherstellen, dass ausscheidende Benutzer bis zum Ende ihres letzten Arbeitstags vollständig aus Systemen und Einrichtungen entfernt werden.

3.3 Verhindern, dass verwaiste Benutzerkonten und nicht zurückgegebene Vermögenswerte Sicherheitsrisiken verursachen.

3.4 Dokumentierte Nachweise über Onboarding-, Versetzungs- und Offboarding-Maßnahmen aufrechterhalten.

3.5 Rechenschaftspflicht durch Checklisten und funktionsübergreifende Rollenklarheit fördern.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer (GM)

4.1.1 Genehmigt Zugriffe für hochprivilegierte Rollen und überwacht das Onboarding- und Offboarding-Programm.

4.1.2 Stellt sicher, dass Ausnahmen begründet sind und Korrekturmaßnahmen ergriffen werden, wenn Prozesse nicht eingehalten werden.

4.2 Office Manager / Personalwesen

4.2.1 Initiiert das Onboarding für Neueinstellungen und informiert die IT über Austritte.

4.2.2 Stellt sicher, dass rechtliche Dokumente (z. B. Geheimhaltungsvereinbarung (NDA)) und Richtlinienbestätigungen abgeschlossen werden.

4.2.3 Pflegt Onboarding-/Offboarding-Checklisten und überwacht die Einhaltung dieser Richtlinie.

[... 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

9.1.1 Diese Richtlinie muss mindestens einmal jährlich durch den Geschäftsführer (GM) sowie die zuständigen Leitungen von Personalwesen und IT überprüft werden.

9.2 Auslöser für eine vorgezogene Überprüfung

9.2.1 Aktualisierungen müssen erfolgen, wenn:

9.2.1.1 neue HR- oder IT-Systeme eingeführt werden

9.2.1.2 ein Wechsel des externen IT-Dienstleisters oder des ausgelagerten HR-Service erfolgt

9.2.1.3 Sicherheitsaudits Prozesslücken aufdecken

9.2.1.4 sich regulatorische Verpflichtungen ändern (z. B. Aktualisierungen der DSGVO)

9.2.1.5 ein kritisches Versagen im Offboarding oder eine Sicherheitsverletzung eintritt

9.3 Versionskontrolle und Genehmigung

9.3.1 Jede Version dieser Richtlinie muss Folgendes enthalten:

9.3.1.1 Versionsnummer und Datum

9.3.1.2 Zusammenfassung der Änderungen

9.3.1.3 Genehmigung durch den Geschäftsführer (GM)

9.3.1.4 archivierte frühere Versionen, die mindestens drei Jahre aufbewahrt werden

9.4 Kommunikation und Bestätigung

9.4.1 Sämtliches Personal, das für Onboarding oder Offboarding verantwortlich ist, muss über Aktualisierungen dieser Richtlinie informiert werden. Jährliche Sensibilisierungs- oder Auffrischungsbriefings sind verpflichtend.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie unterstützt die folgenden Richtlinien und wird durch diese unterstützt:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Stellt Rechenschaftspflicht in Zugriffs- und Onboarding-Prozessen sicher

10.1.2 P4S – Zugriffsrichtlinie: Legt die technische Durchsetzung der rollenbasierten Bereitstellung und Deaktivierung fest

10.1.3 P6S – Risikomanagement-Richtlinie: Bewertet Risiken, die aus Mängeln bei Kontrollen im Onboarding und Offboarding entstehen

10.1.4 P8S – Richtlinie zur Sensibilisierung für Informationssicherheit und Schulung: Verankert Anforderungen an die Einweisung von Beschäftigten beim Onboarding

10.1.5 P30S – Richtlinie zum Management von Informationssicherheitsvorfällen (P30): Behandelt den unterlassenen Entzug von Zugriffsberechtigungen oder den Diebstahl von Vermögenswerten als Informationssicherheitsvorfälle

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.2 – Legt Anforderungen an die Personalsicherheit fest

11.1.2 Klausel 7.2 – Schreibt Sensibilisierungsschulungen für neue Beschäftigte vor

11.2 ISO/IEC 27002

11.2.1 Maßnahmen 6.2 und 6.5 – Beschreiben Sicherheitspraktiken für Onboarding und Offboarding im Beschäftigungskontext

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Verfahren zur Beendigung von Beschäftigungsverhältnissen einschließlich Kontodeaktivierung

11.3.2 AC-2 – Stellt das Management des Zugriffslebenszyklus für Benutzerzugriffe sicher

11.3.3 PL-4 – Verlangt die Planung personeller Übergänge

11.4 EU DSGVO

11.4.1 Artikel 32 – Gewährleistet angemessene Sicherheit während und nach dem Beschäftigungsverhältnis, insbesondere beim Zugriff auf personenbezogene Daten

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(h) – Verlangt Kontrollen zur Personalsicherheit und zum Zugriffslebenszyklus

11.6 EU DORA

11.6.1 Artikel 12 – Verlangt von regulierten Finanzunternehmen die Kontrolle des Personalzugriffs auf IKT-Systeme, einschließlich Verfahren zum Entzug von Zugriffsrechten

11.7 COBIT 2019

11.7.1 APO07 Personalmanagement – Legt Sicherheitsanforderungen für den Personallebenszyklus fest

11.7.2 DSS01 – Betrieb verwalten: Umfasst die Kontrolle des logischen und physischen Zugriffs bei personellen Übergängen