| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P07 | | | | | Dokumenttitel:<br>**Richtlinie für Onboarding und Offboarding** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>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 | Klausel 7.2, Klausel 6 | Personalkompetenz, sichere Integration sowie Durchsetzung von Verantwortlichkeiten bei Austritt oder Rollenwechsel. |
| ISO/IEC 27002:2022 | Maßnahmen 6.2, 6.5, 5 | Kontrollen für Onboarding, Zugriffssteuerung und den Personallebenszyklus. |
| NIST SP 800-53 Rev.5 | PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6 | Personalwechsel und Ausscheiden, Prinzip der minimalen Berechtigung, Audit-Protokollierung sowie Zugriffsverwaltung während und nach Personalveränderungen. |
| DSGVO | Artikel 5(1)(f), 25, 32; Erwägungsgrund 39 | Zugriffsbeschränkung, Vertraulichkeit, Schutz und angemessene Kontrollen für personenbezogene Daten von Beschäftigten. |
| NIS2-Richtlinie | Artikel 21(2)(b, c, d) | Maßnahmen zur Personal- und Betriebssicherheit, Eindämmung von Insider-Bedrohungen sowie Lebenszyklusprozesse. |
| DORA | Artikel 5, 8, 9 | Governance, interne IKT-Kontrolle, IKT-Risiken und Vorfallmanagement bei Personalwechseln. |
| COBIT 2019 | APO07 Personalmanagement, BAI08, DSS05 Sicherheitsdienste verwalten, MEA03 | Personalmanagement, Wissensmanagement, Sicherheit und Compliance bei Onboarding und Offboarding. |

**1. Zweck**

1.1 Diese Richtlinie legt standardisierte Verfahren für das Management von Onboarding, Versetzungen und Offboarding für alle Benutzertypen fest.

1.2 Sie stellt die rechtzeitige und sichere Provisionierung sowie den Entzug von Zugriffsberechtigungen für physischen und logischen Zugriff sicher und gewährleistet dabei Vertraulichkeit, Nachvollziehbarkeit sowie die Rückführung und Validierung von Assets.

1.3 Diese Richtlinie mindert Risiken im Zusammenhang mit unbefugtem Zugriff, Datenabfluss und nicht zurückgegebenen Vermögenswerten, indem Kontrollen für Onboarding und Offboarding in HR-, IT- und Sicherheitsprozesse eingebettet werden.

1.4 Sie unterstützt ISO/IEC 27001:2022 Anhang A Maßnahme 6.5, indem sichergestellt wird, dass personelle Sicherheitsverpflichtungen während und nach der Beschäftigung oder Beauftragung durchgesetzt werden.

**2. Geltungsbereich**

2.1 Diese Richtlinie gilt für alle Mitarbeitenden sowie für Auftragnehmer, Berater, Lieferanten und sonstige Dritte, denen Zugriff auf die Systeme, Netzwerke, Einrichtungen oder Daten der Organisation gewährt wird.

**2.2 Sie regelt den vollständigen Lebenszyklus von:**

2.2.1 Onboarding (Einstellung, Beauftragung oder befristete Einbindung)

2.2.2 Versetzungen oder Rollenänderungen

2.2.3 Offboarding (Kündigung, Ruhestand, Beendigung, Vertragsablauf)

**2.3 Die Richtlinie umfasst:**

2.3.1 Logischen Zugriff (Systeme, Anwendungen, Cloud, VPN)

2.3.2 Physischen Zugriff (Ausweise, Schlüssel, Gebäudeeintrittssysteme)

2.3.3 Zugewiesene Assets (Laptops, Telefone, Token, Anmeldeinformationen)

2.3.4 Bestätigung von Richtlinien und Vertraulichkeitsverpflichtungen

2.4 Alle Abteilungen (HR, IT, Facility Management, Asset Management, Sicherheit und Management) sind für die Wahrnehmung ihrer Rolle in den Onboarding- und Offboarding-Workflows verantwortlich.

## 3. Ziele

3.1 Sicherzustellen, dass sämtliches Personal erst dann Zugriff erhält, wenn Sicherheits-, Schulungs- und vertragliche Voraussetzungen erfüllt sind.

3.2 Zugriffsrechte bei Rollenänderungen oder Austritt unverzüglich zu entziehen und organisatorische Assets zurückzuführen.

3.3 Die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) organisatorischer Assets bei Personalwechseln zu wahren.

3.4 Auditierbarkeit und rechtliche Belastbarkeit durch vollständige Aufzeichnungen zu Onboarding- und Austrittsereignissen zu unterstützen.

3.5 Die Exposition gegenüber Insider-Bedrohungen zu reduzieren, indem alle zugriffsbezogenen Ereignisse im Zusammenhang mit Personal überprüft und dokumentiert werden.

3.6 Den Personallebenszyklus der Organisation an risikobasierten Sicherheitspraktiken und regulatorischen Vorgaben auszurichten.

## 4. Rollen und Verantwortlichkeiten

### 4.1 Geschäftsleitung

4.1.1 Genehmigt diese Richtlinie und weist Befugnisse und Ressourcen für Onboarding-, Offboarding- und Zugriffssteuerungsprozesse zu.

4.1.2 Stellt sicher, dass Personalwechsel die Organisation keinem unangemessenen Sicherheits- oder Rechtsrisiko aussetzen.

### 4.2 Human Resources (HR)

4.2.1 Leitet Onboarding- und Offboarding-Workflows für Mitarbeitende ein und benachrichtigt relevante Abteilungen über Änderungen.

4.2.2 Stellt sicher, dass Hintergrundprüfungen, Verträge, Geheimhaltungsvereinbarungen (NDA) und Richtlinienbestätigungen abgeschlossen sind, bevor Zugriff gewährt wird.

4.2.3 Informiert IT sowie Facility Management und Asset Management über das Ausscheiden von Mitarbeitenden gemäß dem Benachrichtigungs-SLA.

4.2.4 Koordiniert sich mit dem Personalwesen und der Rechtsabteilung, um Verpflichtungen nach Beendigung des Beschäftigungsverhältnisses durchzusetzen (z. B. Vertraulichkeitsklauseln).

[ ... 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 Häufigkeit der Richtlinienüberprüfung

#### 9.1.1 Diese Richtlinie muss überprüft werden:

9.1.1.1 Jährlich, oder

9.1.1.2 Nach jedem wesentlichen Vorfall im Zusammenhang mit missbräuchlicher Nutzung von Zugriffsrechten, Verlust von Assets oder Verfahrensversagen

9.1.1.3 Bei Einführung wesentlicher Änderungen an HR- oder IAM-Plattformen

9.1.1.4 Bei regulatorischen oder rechtlichen Änderungen, die Personaldaten oder Verpflichtungen betreffen

### 9.2 Überprüfungsprozess und Verantwortlichkeit

9.2.1 Der ISMS-Manager und der HR-Direktor koordinieren die Überprüfung unter Einbeziehung von IT-Sicherheit, Personalwesen und Rechtsabteilung sowie Compliance.

9.2.2 Alle Änderungen müssen von der Geschäftsleitung und dem Informationssicherheitslenkungsausschuss genehmigt werden.

9.2.3 Überarbeitete Versionen müssen an betroffene Abteilungen und Mitarbeitende zur erneuten Bestätigung verteilt werden.

### 9.3 Dokumentenlenkung und Aufbewahrung

9.3.1 Diese Richtlinie muss Folgendes enthalten:

9.3.2 Versionskontrolle, Versionshistorie und Wirksamkeitsdatum

9.3.3 Verantwortlichen Eigentümer und Prüfer

9.3.4 Richtlinienklassifizierung und Genehmigungsnachweis

9.3.5 Veraltete Versionen sind gemäß der Dokumentenmanagement-Richtlinie mindestens 3 Jahre zu archivieren.

## 10. Zugehörige Richtlinien und Verknüpfungen

10.1.1 Diese Richtlinie ist direkt verknüpft mit:

10.1.2 P1 – Informationssicherheitsrichtlinie: Legt die Sicherheitsziele der Organisation fest, einschließlich der Governance von Personalzugriffen.

10.1.3 P4 – Zugriffsrichtlinie: Legt operative Anforderungen für die Vergabe und den Entzug von System- und physischen Zugriffen auf Basis von Onboarding- und Offboarding-Auslösern fest.

10.1.4 P3 – Richtlinie zur zulässigen Nutzung: Verlangt eine Bestätigung während des Onboardings und unterstützt die Durchsetzung nach dem Austritt.

10.1.5 P6 – Risikomanagement-Richtlinie: Stellt sicher, dass Risiken im Zusammenhang mit Benutzerzugriffen und Übergängen im Einklang mit den Grundsätzen des ISMS bewertet und behandelt werden.

10.1.6 P11 – Richtlinie für Benutzerkonten- und Berechtigungsmanagement: Regelt die technischen Kontrollen für Provisionierung und Entzug von Zugriffsberechtigungen zur Unterstützung dieser Richtlinie.

10.2 Diese Richtlinien bilden ein integriertes Kontrollsystem für das sichere und nachvollziehbare Management von Ereignissen im Personallebenszyklus.

## 11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Rahmenwerken für Sicherheit, Datenschutz und IT-Governance ausgerichtet, um sicherzustellen, dass Onboarding- und Offboarding-Prozesse sicher, nachvollziehbar und im Einklang mit rechtlichen und organisatorischen Anforderungen sind.

**11.2 ISO/IEC 27001:**

11.2.1 Klausel 7.2 – Kompetenz und Klausel 6.2 – Informationssicherheitsziele: Diese Richtlinie unterstützt den Aufbau personeller Kompetenz und die sichere Integration von Personen in Rollen, in denen sie ISMS-Ziele beeinflussen.

11.2.2 Anhang A Maßnahme 6.5 – Verantwortlichkeiten nach Beendigung oder Änderung des Beschäftigungsverhältnisses: Diese Richtlinie setzt Kontrollen über verbleibende Zugriffsrechte, Datenaufbewahrung und vertragliche Verpflichtungen beim Ausscheiden vollständig durch.

11.2.3 Anhang A Maßnahme 5.9 – Überprüfung und 6.2 – Beschäftigungsbedingungen: Die Onboarding-Verfahren beinhalten Hintergrundprüfungen und Mechanismen zur Richtlinienbestätigung im Einklang mit diesen Vorgaben.

**11.3 NIST SP 800-53 Rev.5:**

11.3.1 PS-4 (Beendigung von Beschäftigungsverhältnissen) und PS-5 (Versetzung von Personal): Diese Richtlinie setzt die strukturierte Entfernung oder Änderung von Zugriffsrechten, Zutrittsausweisen und Assets durch.

11.3.2 AC-2 (Kontenmanagement) und AC-6 (Prinzip der minimalen Berechtigung): Die Vorgaben stellen sicher, dass Zugriffe rollenbezogen sind und unverzüglich entzogen werden, sobald sie nicht mehr erforderlich sind.

11.3.3 IA-4 (Kennungsmanagement) und IA-5 (Management von Authentifikatoren): Unterstützt das sichere Management von Anmeldeinformationen während und nach Personaländerungen.

11.3.4 CM-5 (Zugriffsbeschränkungen für Änderungen): Verhindert unbefugte Änderungen nach Austritt durch den Entzug erweiterter Zugriffsrechte.

11.3.5 AU-2 und AU-6: Protokollierung und Nachvollziehbarkeit von Zugriffsereignissen werden durch IAM und die Integration des Audit-Trails gestärkt.

**11.4 DSGVO (2016/679):**

11.4.1 Artikel 5(1)(f): Schützt personenbezogene Daten vor unbefugtem Zugriff; dies wird hier durch den Entzug von Benutzerzugriffen beim Offboarding umgesetzt.

11.4.2 Artikel 32: Verlangt angemessene technische und organisatorische Kontrollen zum Schutz personenbezogener Daten während des Beschäftigungslebenszyklus.

11.4.3 Artikel 25 – Datenschutz durch Technikgestaltung: Stellt sicher, dass Onboarding und Offboarding Datenminimierung, Aufbewahrung und rechtmäßige Zugriffssteuerung integrieren.

11.4.4 Erwägungsgrund 39: Betont Zugriffsbeschränkung und Vertraulichkeit, die durch die Struktur dieser Richtlinie unterstützt werden.

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

11.5.1 Artikel 21(2)(b, c, d): Verlangt Maßnahmen zur Personal- und Betriebssicherheit zur Adressierung von Zugriffssteuerung, Eindämmung von Insider-Bedrohungen und Lebenszyklusprozessen, die sämtlich in dieser Richtlinie berücksichtigt sind.

**11.6 DORA (2022/2554):**

11.6.1 Artikel 5 – Governance und interne Kontrolle: Diese Richtlinie unterstützt die interne IKT-Governance im Zusammenhang mit personellen Risiken und Zugriffsverwaltung.

11.6.2 Artikel 8 – IKT-Risikomanagement: Wendet Kontrollen auf Personalwechsel an, die kritische Assets oder regulierte Umgebungen gefährden könnten.

11.6.3 Artikel 9 – Klassifizierung und Management von Vorfällen: Stellt sicher, dass Verstöße im Zusammenhang mit Austritten meldepflichtig sind und durch ordnungsgemäßen Entzug von Zugriffsberechtigungen sowie Asset-Handhabung gemindert werden.

**11.7 COBIT 2019:**

11.7.1 APO07 Personalmanagement – Managed Human Resources: Definiert Rollen, Verantwortlichkeiten und Lebenszyklusmaßnahmen für Onboarding und Offboarding in Ausrichtung auf Governance-Ziele.

11.7.2 BAI08 – Wissensmanagement: Stärkt die Dokumentation von Verfahren, die Wissensbewahrung und die Kontrollübergabe am Ende des Beschäftigungsverhältnisses.

11.7.3 DSS05 Sicherheitsdienste verwalten – Managed Security Services: Erzwingt Benutzerdeaktivierung, Asset-Kontrolle und Nachvollziehbarkeit bei Rollenübergängen.

11.7.4 MEA03 – Überwachen, Evaluieren und Beurteilen der Einhaltung: Stellt sicher, dass Onboarding- und Offboarding-Kontrollen bei internen und externen Audits bewertet werden.