					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P34					Dokumenttitel: **Richtlinie für mobile Geräte und Bring Your Own Device (BYOD)**							
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/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Wendet Sicherheitsmaßnahmen und Compliance-Verpflichtungen an
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Stellt detaillierte Maßnahmen für die Verwaltung mobiler Geräte bereit
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Zugriffskontrolle, Fernzugriff, Konfiguration und Sicherheitsanforderungen für mobile Geräte
EU-DSGVO	5(1)(f), 25, 32	Verbindliche Anforderungen an Datenschutz, Datenverschlüsselung und Sicherheit der Verarbeitung
EU NIS2	21(2)(d)	Technische und organisatorische Schutzmaßnahmen für mobilen Zugriff
EU DORA	9, 10	IKT-Risikomanagement und Sicherheitsanforderungen für mobile Geräte
COBIT 2019	APO13.02, DSS01.04, BAI09	Informationssicherheitspläne, Asset-Konfiguration und Kontrollen für mobile Umgebungen

1. Zweck

1.1 Diese Richtlinie legt die Sicherheits-, Compliance- und Betriebsanforderungen für die Nutzung mobiler Geräte und persönlicher Technologien (Bring Your Own Device (BYOD)) beim Zugriff auf Systeme, Anwendungen oder Daten der Organisation fest.

1.2 Sie dient der Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Unternehmensinformationen, auf die über mobile Endgeräte zugegriffen oder die über diese verarbeitet werden, einschließlich Smartphones, Tablets, Laptops und Hybridgeräten.

1.3 Sie schreibt zudem die technischen und prozessualen Maßnahmen vor, die erforderlich sind, um Risiken wie Datenabfluss, unbefugten Zugriff, Verlust oder Diebstahl von Geräten sowie die Kompromittierung mobiler Anwendungen zu mindern.

1.4 Diese Richtlinie unterstützt die Einhaltung regulatorischer und vertraglicher Anforderungen und ermöglicht zugleich eine sichere mobile Arbeitsfähigkeit für Mitarbeiter, Auftragnehmer und autorisierte Dritte.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für sämtliches Personal, einschließlich Mitarbeiter, Auftragnehmer, Praktikanten und externe IT-Dienstleister, das mobile Geräte für den Zugriff auf Unternehmensdaten, Systeme, Anwendungen oder Kommunikationsplattformen nutzt.

2.2 Sie umfasst alle mobilen Endgeräte, einschließlich, aber nicht beschränkt auf:

2.2.1 Smartphones und Tablets (iOS, Android usw.)

2.2.2 Laptops und Ultrabooks (Windows, macOS, Linux)

2.2.3 Wearables und hybride intelligente Geräte mit Funktionen zur Datensynchronisierung

2.3 Sie gilt unabhängig davon, ob es sich um unternehmenseigene Geräte oder privat genutzte Geräte im Rahmen einer BYOD-Vereinbarung handelt.

2.4 Die Richtlinie umfasst alle Zugriffswege, einschließlich VPN, virtueller Desktops, Cloud-Anwendungen, E-Mail, Kollaborationsplattformen (z. B. SharePoint, Teams) und Werkzeuge zur Dateisynchronisierung (z. B. OneDrive, Dropbox, sofern autorisiert).

2.5 Sie gilt für die Nutzung im Remote-Arbeitskontext, an Unternehmensstandorten, auf Reisen oder in hybriden Arbeitsmodellen.

3. Ziele

3.1 Reduzierung des Risikos einer Datenkompromittierung, eines Datenabflusses oder Datenverlusts infolge einer unsicheren Nutzung mobiler Geräte.

3.2 Durchsetzung konsistenter und verbindlicher Sicherheitsmaßnahmen über alle mobilen Endgeräte hinweg, unabhängig vom Eigentumsmodell (Unternehmensgerät oder BYOD).

3.3 Sicherstellung, dass die Nutzung mobiler Geräte den Anforderungen der ISO/IEC 27001 und anderer anwendbarer regulatorischer Rahmenwerke für Datenschutz, Datensicherheit und Cybersicherheit entspricht.

3.4 Ermöglichung der sicheren Integration mobiler Geräte in die betrieblichen, kommunikativen und kollaborativen Arbeitsabläufe der Organisation.

3.5 Festlegung klar definierter Verantwortlichkeiten und Prozesse für das Mobile Device Management (MDM), einschließlich Registrierung, Fernlöschung, Verschlüsselung, Authentifizierung und Überwachung.

3.6 Schutz der Datenschutzrechte von Personen, die ihre eigenen Geräte nutzen, bei gleichzeitiger Wahrung der sensiblen Informationen der Organisation.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO) / Leitung Informationssicherheit

4.1.1 Legt Richtlinien und technische Standards für die Nutzung mobiler Geräte und BYOD fest.

4.1.2 Überwacht die Einhaltung, die Reaktion auf Sicherheitsvorfälle und das Ausnahmemanagement für Maßnahmen zum Schutz mobiler Geräte.

4.1.3 Stimmt sich mit Personalwesen und Rechtsabteilung ab, um eine rechtssichere und organisatorisch abgestimmte Durchsetzung sicherzustellen.

4.2 IT-Administrator / MDM-Administrator

4.2.1 Verwaltet die Bereitstellung, Registrierung und Konfiguration mobiler Geräte über MDM-Lösungen.

4.2.2 Setzt Maßnahmen auf Geräteebene durch (z. B. Verschlüsselung, PIN-Codes, Anwendungskontrollen).

4.2.3 Führt bei Bedarf Fernlöschungen, Gerätesperrungen und den Entzug von Zugriffsrechten durch.

[... 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 CISO oder einen benannten Informationssicherheitsmanager zu überprüfen, um die Ausrichtung an Folgendem sicherzustellen:

9.1.1 Änderungen an mobilen Betriebssystemplattformen, MDM-Technologien oder Authentifizierungsstandards

9.1.2 regulatorische oder vertragliche Änderungen, die den Schutz mobiler Daten betreffen (z. B. DSGVO, DORA, NIS2)

9.1.3 Überarbeitungen der Maßnahmenkataloge von ISO/IEC 27001:2022, ISO/IEC 27002:2022 oder NIST SP 800-53 Rev.5

9.1.4 Rückmeldungen aus Audits, Nachbetrachtungen von Sicherheitsvorfällen oder Mitarbeitermeldungen

9.2 Außerplanmäßige Überprüfungen können ausgelöst werden durch:

9.2.1 Sicherheitsvorfälle im Zusammenhang mit mobilen Geräten oder BYOD-Plattformen

9.2.2 Herstellerhinweise zu Schwachstellen mit hohem Risiko in unterstützten Plattformen

9.2.3 die Einführung neuer mobiler Anwendungen oder Kollaborationsplattformen für den Geschäftsbetrieb

9.3 Aktualisierungen der Richtlinie müssen:

9.3.1 in der Versionshistorie der Richtlinie dokumentiert werden,

9.3.2 an sämtliches Personal und betroffene Auftragnehmer kommuniziert werden,

9.3.3 von allen BYOD-Benutzern durch eine aktualisierte Bestätigung erneut bestätigt werden.

9.4 Alle Überprüfungen und Überarbeitungen müssen formell von der Geschäftsleitung genehmigt und im Register für Richtlinienänderungen protokolliert werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie steht in Wechselwirkung mit mehreren zentralen Richtlinien im Rahmen des Informationssicherheitsmanagementsystems (ISMS) der Organisation. Wesentliche Verknüpfungen sind:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt die übergeordneten Governance-Grundsätze für alle Informationssicherheitsmaßnahmen fest, einschließlich der Maßnahmen für die Nutzung mobiler Geräte.

10.1.2 P3 – Richtlinie zur zulässigen Nutzung: Definiert zulässige Verhaltensweisen und Beschränkungen bei der Nutzung von Technologien, die unmittelbar auch für mobilen Zugriff und BYOD gelten.

10.1.3 P9 – Richtlinie für Remote-Arbeit: Regelt zusätzliche Sicherheitsverpflichtungen für mobile Arbeitsumgebungen und ergänzt die in dieser Richtlinie festgelegten mobilitätsspezifischen Maßnahmen.

10.1.4 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Regelt, wie Daten auf mobilen Geräten entsprechend ihrer Klassifizierungsstufe zu handhaben sind, mit Auswirkungen auf Speicherung, Übertragung und Durchsetzung der Verschlüsselung.

10.1.5 P22 – Richtlinie zur Protokollierung und Überwachung: Unterstützt die Erfassung und Überprüfung von Zugriffsprotokollen für mobile Zugriffe zur Erkennung von Anomalien oder Verstößen.

10.1.6 P30 – Incident-Response-Richtlinie (P30): Regelt, wie mobilitätsbezogene Vorfälle (z. B. Geräteverlust, unbefugter Zugriff) behandelt und eskaliert werden.

10.1.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Bildet die Grundlage für regelmäßige Prüfungen der Einhaltung mobiler Sicherheitsanforderungen, einschließlich der Einhaltung der BYOD-Richtlinie.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Rahmenwerken für Cybersicherheit und rechtlichen Verpflichtungen ausgerichtet, um die sichere Nutzung mobiler Geräte und persönlicher Technologien (BYOD) in Unternehmensumgebungen sicherzustellen.

11.2 ISO/IEC 27001:

11.2.1 Maßnahme 5.10 – Zulässige Nutzung von Informationswerten: Fordert Maßnahmen für die verantwortungsvolle Nutzung von Informationswerten, einschließlich mobiler Geräte.

11.2.2 Maßnahme 6.7 – Remote-Arbeit: Regelt sichere Praktiken beim Zugriff auf Systeme außerhalb der Unternehmensräumlichkeiten.

11.2.3 Maßnahme 8.1 – Endgeräte: Verlangt risikobasierte Maßnahmen für mobile Endgeräte und BYOD-Konfigurationen.

11.2.4 Maßnahme 5.14 – Informationsübertragung: Erzwingt den Schutz von Informationen, die über mobile Kanäle übertragen werden.

11.3 ISO/IEC 27002:2022 – Maßnahmen 5.10 bis 5.13:

11.3.1 Die Maßnahmen 5.10 bis 5.13 legen fest, wie mobiler Zugriff, Verschlüsselung, Überwachung und Verlustminderung innerhalb eines Informationssicherheitsmanagementsystems (ISMS) durchzusetzen sind. Diese Maßnahmen enthalten detaillierte Umsetzungshinweise zur Absicherung mobiler Endgeräte, zur Durchsetzung von Containerisierung, zur Überwachung der Geräteintegrität und zur Sicherstellung datenschutzgerechter Konfigurationen für die BYOD-Nutzung.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Zugriffskontrolle für mobile Geräte: Definiert Basisschutzmaßnahmen, einschließlich Verschlüsselung, Authentifizierung und MDM-Durchsetzung.

11.4.2 AC-17 – Fernzugriff: Verlangt sichere Authentifizierung und Sitzungsschutz für mobile Benutzer mit Fernzugriff.

11.4.3 CM-7 – Prinzip der minimalen Funktionalität: Unterstützt die Entfernung unnötiger Anwendungen und Funktionen von mobilen Endgeräten zur Risikoreduzierung.

11.4.4 MP-5 – Schutz beim Transport von Medien: Regelt die sichere Übertragung von Daten von mobilen Systemen an externe oder Cloud-Ziele.

11.4.5 SC-12 – Einrichtung kryptografischer Schlüssel: Verlangt die Nutzung sicherer kryptografischer Protokolle für mobile Kommunikation und Speicherung.

11.5 EU-DSGVO (2016/679):

11.5.1 Artikel 5(1)(f) – Integrität und Vertraulichkeit: Verlangt, dass Organisationen personenbezogene Daten auf mobilen Geräten gegen unbefugten oder unrechtmäßigen Zugriff schützen.

11.5.2 Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Verlangt, dass Datenschutz in BYOD- und MDM-Prozesse eingebettet wird.

11.5.3 Artikel 32 – Sicherheit der Verarbeitung: Erzwingt risikobasierte Maßnahmen (z. B. Verschlüsselung, Authentifizierung, Zugriffskontrolle) für personenbezogene Daten auf mobilen Plattformen.

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

11.6.1 Artikel 21(2)(d): Verlangt, dass mobiler Zugriff auf kritische Systeme und Informationen durch geeignete technische und organisatorische Maßnahmen wie Endgerätekontrolle, Verschlüsselung und Überwachung geschützt wird.

11.7 EU DORA (2022/2554):

11.7.1 Artikel 9 – Rahmenwerk für das IKT-Risikomanagement: Verlangt von Unternehmen des Finanzsektors, mobile und Fernzugriffsrisiken als Teil der operativen Resilienz zu mindern.

11.7.2 Artikel 10 – Sicherheitsanforderungen an IKT-Systeme: Verlangt eine sichere mobile Architektur sowie Überwachungs- und Reaktionsmechanismen für von mobilen Geräten ausgehende Cyberbedrohungen.

11.8 COBIT 2019:

11.8.1 APO13.02 – Einen Informationssicherheitsplan aufstellen und aufrechterhalten: Verlangt, dass die Nutzung mobiler Geräte, einschließlich BYOD, in die Sicherheitsstrategien der Organisation integriert wird.

11.8.2 DSS01.04 – Asset-Konfiguration und -Integrität verwalten: Gilt für Konfigurationskontrolle und sichere Bereitstellung mobiler Geräte.

11.8.3 BAI09.01 – Kontrollen einrichten und aufrechterhalten: Unterstützt die Umsetzung technischer und prozessualer Schutzmaßnahmen für sichere mobile und Remote-Betriebsabläufe.