					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P34S					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/Verordnung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 5.2, 6.1, 6.2, 8	Allgemeine Anforderungen an das Informationssicherheitsmanagementsystem und Kontrollen für mobile Geräte/BYOD
ISO/IEC 27002:2022	Maßnahmen 5.10–5.13	Detaillierte Maßnahmen für mobile Geräte/BYOD und Fernzugriff
NIST SP 800-53 Rev. 5	AC-19, AC-20, CM-6, MP-7	Bundesweite Kontrollen für Geräte, Medien und Konfigurationen
DSGVO	Artikel 5(1)(f)	Schutz personenbezogener Daten auf mobilen Endgeräten
NIS2	Artikel 21(2)(d)	Schutz geschäftskritischer Geräte (einschließlich BYOD)
DORA	Artikel 9, 10	Anforderungen an IKT-Risikomanagement und Betriebskontinuität für mobile Endgeräte
COBIT 2019	APO13, DSS01, DSS05	Kontrollen für IT-Governance, Betrieb und Sicherheitsdienste

1. Zweck

1.1. Diese Richtlinie legt die verbindlichen Sicherheitsanforderungen für die Nutzung mobiler Geräte – einschließlich Smartphones, Tablets und Laptops – beim Zugriff auf Unternehmensinformationen, Systeme oder Dienste fest.

1.2. Sie regelt außerdem die Nutzung von Bring Your Own Device (BYOD), um sicherzustellen, dass Kunden- und Unternehmensdaten unabhängig von den Eigentumsverhältnissen des Geräts geschützt sind.

1.3. Die Richtlinie stellt einheitliche Schutzmaßnahmen für den mobilen Zugriff sicher, unterstützt die Ziele der ISO/IEC-27001-Zertifizierung und verhindert Datenverlust oder Kompromittierung durch verlorene, gestohlene oder missbräuchlich genutzte mobile Endgeräte.

1.4. Sie stellt sicher, dass in KMU ohne dedizierte IT-Teams sowohl technische als auch organisatorische Schutzmaßnahmen für die mobile Nutzung angewendet werden, einschließlich in Remote-Arbeitsumgebungen und bei cloudbasierten Diensten.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Mitarbeitenden, Auftragnehmer, Praktikanten und Dienstleister, die:

2.1.1. ein mobiles Gerät nutzen, um auf Unternehmensdaten oder Systeme zuzugreifen, diese zu verarbeiten oder zu speichern,

2.1.2. eine Verbindung zu Unternehmensdiensten herstellen, einschließlich E-Mail, gemeinsamen Ordnern, Cloud-Anwendungen oder internen Systemen über VPN.

2.2. Sie umfasst:

2.2.1. alle mobilen Geräte: Smartphones, Tablets, Laptops (vom Unternehmen bereitgestellt oder persönliche Bring Your Own Device (BYOD)-Geräte),

2.2.2. alle Betriebssysteme (z. B. iOS, Android, Windows, macOS),

2.2.3. alle Standorte (Büro, Zuhause, Remote-Arbeitsplatz, öffentliche Bereiche).

2.3. Die Richtlinie gilt in allen Arbeitsumgebungen und ist unabhängig von den Eigentumsverhältnissen des Geräts verbindlich umzusetzen.

3. Ziele

3.1. Datenverlust verhindern: Sicherstellen, dass die mobile Nutzung sensible Unternehmens- oder Kundendaten keinem unbefugten Zugriff, Diebstahl oder Missbrauch aussetzt.

3.2. Klare Regeln für Bring Your Own Device (BYOD) festlegen: Verbindliche Bedingungen für die Nutzung persönlicher Geräte zu geschäftlichen Zwecken vorgeben und dabei rechtliche sowie technische Schutzmaßnahmen sicherstellen.

3.3. Regulatorische Anforderungen erfüllen: Anforderungen aus ISO/IEC 27001, DSGVO, NIS2 und anderen rechtlichen Verpflichtungen durch verbindliche Sicherheitspraktiken für mobile Geräte umsetzen.

3.4. Betriebsrisiken minimieren: Die Wahrscheinlichkeit betrieblicher Störungen durch missbräuchliche Nutzung, Kompromittierung oder Ausfall mobiler Geräte verringern.

3.5. Vertrauen von Kunden wahren: Gegenüber Kunden und Partnern nachweisen, dass ihre Daten auch dann geschützt bleiben, wenn auf sie über mobile oder persönliche Geräte zugegriffen wird.

4. Rollen und Verantwortlichkeiten

4.1. General Manager (GM):

4.1.1. Trägt die Gesamtverantwortung für diese Richtlinie.

4.1.2. Genehmigt jede Nutzung des mobilen Zugriffs und von Bring Your Own Device (BYOD) auf Unternehmenssysteme.

4.1.3. Stellt sicher, dass BYOD-Vereinbarungen unterzeichnet, aufbewahrt und überwacht werden.

4.1.4. Verifiziert, dass externe IT-Dienstleister die erforderlichen Schutzmaßnahmen für mobile Geräte umsetzen.

4.2. Benannte Mitarbeitende oder IT-Support:

4.2.1. Unterstützen bei Einrichtung, Erfassung und Konfiguration mobiler Geräte, die für die Arbeit genutzt werden.

4.2.2. Setzen gerätebezogene Zugriffskontrollen, Anwendungseinschränkungen und Überwachungsrichtlinien um.

4.2.3. Unterstützen die Reaktion auf Sicherheitsvorfälle im Zusammenhang mit mobilen Geräten (verlorene, gestohlene oder kompromittierte Geräte).

[... 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. Der General Manager (GM) muss diese Richtlinie mindestens einmal innerhalb von 12 Monaten überprüfen.

9.1.2. Im Rahmen der Überprüfung ist die fortlaufende Ausrichtung an den Anforderungen der ISO/IEC 27001, an der Weiterentwicklung mobiler Technologien sowie an Änderungen der Geschäftsabläufe zu verifizieren.

9.1.3. Aktualisierungen müssen außerdem jüngste Vorfälle, Auditergebnisse oder regulatorische Entwicklungen (z. B. DSGVO, NIS2, DORA) berücksichtigen.

9.2. Auslösende Ereignisse für eine außerplanmäßige Überprüfung

9.2.1. Diese Richtlinie muss unverzüglich aktualisiert werden, wenn eines der folgenden Ereignisse eintritt:

9.2.1.1. Wesentlicher Sicherheitsvorfall im Zusammenhang mit mobilen Geräten (z. B. Datenschutzverletzung durch ein verlorenes oder kompromittiertes Gerät)

9.2.1.2. Änderung der unterstützten Plattformen oder Werkzeuge für das Management mobiler Geräte

9.2.1.3. Rechtliche oder regulatorische Änderung, die die Nutzung persönlicher Geräte oder den Datenschutz betrifft

9.2.1.4. Einführung neuer Anwendungen, Dienste oder Werkzeuge von Drittparteien, die auf mobilen Geräten genutzt werden

9.3. Dokumentation von Änderungen

9.3.1. Alle Überprüfungen und Aktualisierungen müssen dokumentiert werden, einschließlich des Datums der Überprüfung, der vorgenommenen Änderungen und der Genehmigung durch den GM.

9.3.2. Eine Versionshistorie muss für Audit-Zwecke aufbewahrt werden.

9.4. Kommunikation und Zugriff

9.4.1. Der GM muss sicherstellen, dass alle Benutzer (Mitarbeitende, Auftragnehmer, Dritte) über Änderungen informiert werden.

9.4.2. Aktualisierte Fassungen müssen leicht zugänglich bereitgestellt werden, beispielsweise in gemeinsamen Ordnern oder auf internen Plattformen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist Bestandteil des übergreifenden Richtlinienwerks zur Informationssicherheit für KMU und muss zusammen mit den folgenden Richtlinien umgesetzt werden:

10.1.1. P4S – Richtlinie zur Zugriffskontrolle: Legt Anforderungen für die Verwaltung des sicheren Zugriffs auf Systeme fest, einschließlich solcher, auf die über mobile Geräte zugegriffen wird. Sie setzt Passwortsicherheit und Sitzungsmanagement durch.

10.1.2. P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass Benutzer in der sicheren Nutzung mobiler Geräte, der Vorfallmeldung und den Bedingungen für Bring Your Own Device (BYOD) geschult werden.

10.1.3. P17S – Richtlinie zu Datenschutz und Privatsphäre: Legt die DSGVO-konforme Handhabung personenbezogener Daten und Unternehmensdaten auf mobilen Plattformen fest, insbesondere wenn persönliche Geräte für die Arbeit genutzt werden.

10.1.4. P9S – Richtlinie für Remote-Arbeit: Stimmt die Erwartungen an die mobile Nutzung bei der Arbeit außerhalb des Standorts oder von zu Hause aus ab, einschließlich Vorgaben zur Gerätehandhabung und Schutzmaßnahmen für den Netzwerkzugriff.

10.1.5. P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle: Stellt das Rahmenwerk für die Reaktion auf Vorfälle im Zusammenhang mit mobilen Geräten bereit, einschließlich kompromittierter oder verlorener Geräte.

10.2. Diese zugehörigen Richtlinien bilden zusammen ein vollständiges Maßnahmenpaket für die Sicherheit mobiler Geräte in KMU ohne dediziertes IT-Personal und stellen Durchsetzbarkeit, Transparenz und Zertifizierungsfähigkeit sicher.

11. Referenzstandards und Rahmenwerke

11.1. Diese Richtlinie unterstützt die vollständige Ausrichtung an den folgenden Sicherheits- und Compliance-Standards:

11.2. ISO/IEC 27001:

11.2.1. Klausel 5.1 – Führung und Verpflichtung: Stellt Managementaufsicht und Rechenschaftspflicht für mobilen Zugriff und Bring Your Own Device (BYOD) sicher.

11.2.2. Klausel 6.1 – Maßnahmen zum Umgang mit Risiken: Verlangt, dass Risiken der mobilen Sicherheit bewertet und behandelt werden.

11.2.3. Klausel 8.1 – Operative Planung und Steuerung: Fordert einheitliche Verfahren für den mobilen Zugriff zum Schutz geschäftlicher Daten.

11.3. ISO/IEC 27002:

11.3.1. Maßnahmen 5.10 (Nutzung mobiler Geräte), 5.11 (Telearbeit), 5.12 (Fernzugriff) und 5.13 (Bring Your Own Device (BYOD)): Geben Umsetzungsleitlinien für die Steuerung von Geräterisiken im Kontext kleiner Unternehmen vor.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. AC-19 – Zugriffskontrolle für mobile Geräte: Verlangt Sicherheitseinstellungen für genehmigte mobile Nutzung.

11.4.2. AC-20 – Nutzung externer Systeme: Regelt die Risiken von Bring Your Own Device (BYOD) und Fernzugriff.

11.4.3. CM-6 – Konfigurationseinstellungen: Setzt sichere Standard- und individuelle Einstellungen auf mobilen Plattformen durch.

11.4.4. MP-7 – Mediennutzung: Behandelt die ordnungsgemäße Nutzung und Einschränkungen für mobile Speichermedien und den Datenzugriff.

11.5. DSGVO (2016/679):

11.5.1. Artikel 5(1)(f) – Integrität und Vertraulichkeit: Verlangt Datenschutz durch eine angemessene Sicherheit personenbezogener Daten, insbesondere auf mobilen Plattformen.

11.5.2. Artikel 32 – Sicherheit der Verarbeitung: Verpflichtet zur Anwendung geeigneter technischer und organisatorischer Maßnahmen zum Schutz von Daten, auf die über mobile Geräte zugegriffen oder die dort gespeichert werden.

11.6. NIS2-Richtlinie (2022/2555):

11.6.1. Artikel 21(2)(d) – Maßnahmen zur Gerätesicherheit: Verlangt Sicherheitskontrollen für Hardware und Software, die für den Zugriff auf kritische Geschäftssysteme verwendet werden, einschließlich persönlicher Geräte.

11.7. DORA (2022/2554):

11.7.1. Artikel 9 – Rahmenwerk für das IKT-Risikomanagement: Verlangt den Schutz mobiler Endgeräte, die für kritische Geschäftskommunikation und Cloud-Dienste verwendet werden.

11.7.2. Artikel 10 – IKT-Aufrechterhaltung des Geschäftsbetriebs: Stellt die fortlaufende sichere Verfügbarkeit des Zugriffs auf Geschäftssysteme auch während Störungen oder bei Remote-Arbeit sicher.

11.8. COBIT 2019:

11.8.1. APO13 – Sicherheitsmanagement: Verlangt, dass die Organisation Richtlinien für mobile Geräte und Bring Your Own Device (BYOD) entsprechend dem Unternehmensrisiko durchsetzt.

11.8.2. DSS01 – Betriebsmanagement: Stellt die technische Umsetzung sicherer Zugriffsmechanismen sicher.

11.8.3. DSS05 – Sicherheitsdienste verwalten: Regelt die Einbindung von Drittparteien bei der Aufrechterhaltung sicherer mobiler Umgebungen und der Koordination der Reaktion auf Sicherheitsvorfälle.