					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P09					Dokumenttitel: **Richtlinie für Remote-Arbeit**							
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**

1. Zweck

1.1 Diese Richtlinie legt verbindliche Anforderungen für die sichere Durchführung von Remote-Arbeit fest, einschließlich der Nutzung von Systemen der Organisation, des Zugriffs auf Daten sowie der Ausführung von Arbeitsaufgaben außerhalb der Unternehmensstandorte.

1.2 Sie gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Informationswerten, auf die remote zugegriffen wird, und etabliert Kontrollen zur Minderung von Risiken in verteilten Arbeitsumgebungen.

1.3 Die Richtlinie erfüllt Anhang A Maßnahme 6.7 der ISO/IEC 27001:2022 durch die Umsetzung technischer und prozessualer Schutzmaßnahmen, die auf Bedingungen der Remote-Arbeit zugeschnitten sind.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für sämtliches Personal, das zur Remote-Arbeit berechtigt ist, einschließlich:

2.1.1 Mitarbeitende (Vollzeit, Teilzeit, vertraglich gebunden)

2.1.2 Externe Dienstleister, Berater und Lieferanten

2.1.3 Zeitarbeitskräfte und projektbezogen eingesetztes Personal mit genehmigtem Fernzugriff

2.2 Sie umfasst:

2.2.1 Den Zugriff auf Systeme der Organisation über VPN oder genehmigte Fernzugriffswerkzeuge

2.2.2 Den Umgang mit sensiblen und regulierten Informationen außerhalb gesicherter Einrichtungen

2.2.3 Die Nutzung organisationseigener Geräte oder von Bring Your Own Device (BYOD)-Ausstattung

2.2.4 Physischen und logischen Zugriff sowie Schutzmaßnahmen in Remote-Umgebungen

2.3 Die Richtlinie gilt in allen geografischen Regionen und Zeitzonen, in denen die Organisation Remote-Arbeit zulässt, unabhängig davon, ob diese regelmäßig, ad hoc oder im Rahmen von Maßnahmen zur Geschäftskontinuität erfolgt.

3. Ziele

3.1 Sicherzustellen, dass nur autorisierte Personen remote auf interne Systeme und Informationen zugreifen können.

3.2 Die Durchsetzung von Verschlüsselung, Multi-Faktor-Authentifizierung und Endpunktschutz über alle Fernzugriffspfade hinweg sicherzustellen.

3.3 Ein angemessenes Informationssicherheits-Risikoprofil gegenüber Bedrohungen wie Phishing, Schadsoftware, Datenexfiltration und unbefugter Systemoffenlegung aufrechtzuerhalten.

3.4 Zu regeln, wie sensible Daten in externen Arbeitsumgebungen übertragen, gespeichert oder ausgedruckt werden dürfen.

3.5 Physische Sicherheitsmaßnahmen festzulegen, die die Sichtbarkeit und unbefugte Beobachtung während Remote-Sitzungen reduzieren.

3.6 Internationale regulatorische Anforderungen an den Fernzugriff auf Daten, einschließlich DSGVO, NIS2 und DORA, einzuhalten.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt diese Richtlinie und stellt sicher, dass sie personell und organisatorisch unterstützt sowie in HR-, IT- und Sicherheitsprozesse integriert wird.

4.1.2 Genehmigt die Eignungskriterien der Organisation für Remote-Arbeit und deren Anwendbarkeit auf Geschäftsbereiche.

4.2 CISO / ISMS-Manager

4.2.1 Ist für diese Richtlinie verantwortlich, pflegt sie und stellt ihre Ausrichtung am Risikoprofil sowie an regulatorischen Anforderungen sicher.

4.2.2 Definiert Sicherheitskontrollen für den Fernzugriff (z. B. Verschlüsselung, Endpunktschutz, Sitzungszeitüberschreitungen).

4.2.3 Genehmigt den Umgang mit Ausnahmen und überwacht die Wirksamkeit der Kontrollen.

[... 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 Überprüfung

9.1.1 Diese Richtlinie muss jährlich oder bei Bedarf häufiger überprüft werden, insbesondere bei:

9.1.1.1 Einführung neuer Technologien für den Fernzugriff

9.1.1.2 Erheblicher Ausweitung der Remote-Arbeit (z. B. Initiativen für hybride Arbeitsmodelle)

9.1.1.3 Auftreten neuer Bedrohungen, Schwachstellen oder Vorfälle mit Bezug zu Remote-Umgebungen

9.1.1.4 Änderungen relevanter gesetzlicher oder regulatorischer Rahmenbedingungen

9.2 Verantwortlichkeit und Überprüfungsprozess

9.2.1 Verantwortlich für die Richtlinie ist der CISO. Die Überprüfung ist mit folgenden Stellen zu koordinieren:

9.2.1.1 IT-Betrieb und Architektur

9.2.1.2 HR und Facility Management (hinsichtlich betrieblicher und arbeitsplatzbezogener Auswirkungen)

9.2.1.3 Datenschutzbeauftragter (DPO) (hinsichtlich Datenschutz und grenzüberschreitender Datenkontrollen)

9.2.2 Aktualisierungen der Richtlinie müssen:

9.2.2.1 Vom Informationssicherheitslenkungsausschuss genehmigt werden

9.2.2.2 Sämtlichem betroffenen Personal und Auftragnehmern kommuniziert werden

9.2.2.3 In Onboarding- und Auffrischungsschulungsunterlagen integriert werden

9.3 Dokumentenlenkung und Verteilung

9.3.1 Die Richtlinie muss Versionskontrolle, Inkrafttretensdatum und Versionshistorie enthalten.

9.3.2 Ersetzte Versionen sind gemäß der Dokumentenmanagement-Richtlinie (P14) aufzubewahren.

9.3.3 Überarbeitete Versionen müssen für zur Remote-Arbeit berechtigte Benutzer eine verpflichtende erneute Bestätigung der Richtlinie auslösen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie gilt in Verbindung mit:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt die Grundlage für den sicheren Umgang mit Informationswerten fest und gilt für alle Arbeitsumgebungen einschließlich Remote-Arbeit.

10.1.2 P3 – Richtlinie zur zulässigen Nutzung: Regelt die angemessene Nutzung von Geräten und Systemen der Organisation während Remote-Arbeitssitzungen.

10.1.3 P4 – Richtlinie zur Zugriffskontrolle: Stellt sicher, dass Fernzugriffsberechtigungen dem Prinzip der minimalen Rechtevergabe und angemessenen Authentifizierungsmechanismen folgen.

10.1.4 P6 – Risikomanagement-Richtlinie: Definiert, wie Risiken der Remote-Arbeit innerhalb des ISMS identifiziert, behandelt und überwacht werden.

10.1.5 P12 – Richtlinie zum Asset-Management: Verlangt Inventarisierung und Konfigurationsmanagement für alle remote genutzten Geräte.

10.1.6 P22 – Richtlinie zur Protokollierung und Überwachung: Stellt sicher, dass Remote-Sitzungen gemäß den Compliance-Anforderungen überwacht, auditiert und aufbewahrt werden.

10.1.7 P14 – Richtlinie zur Datenaufbewahrung und Entsorgung: Definiert für Remote-Arbeit relevante Regeln zur Datenverarbeitung, einschließlich Wechselmedien und Geräteentsorgung.

10.2 Diese Richtlinien stellen gemeinsam sicher, dass Remote-Arbeit über alle Funktionen und geografischen Regionen hinweg sicher, konform und durchsetzbar ist.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Rahmenwerken für Sicherheit, Datenschutz und IKT-Risikomanagement ausgerichtet, um sichere, nachvollziehbare und konforme Praktiken der Remote-Arbeit sicherzustellen.

11.2 ISO/IEC 27001

11.2.1 Klausel 6.1.3 – Planung der Risikobehandlung: Diese Richtlinie trägt zur Behandlung von Risiken im Zusammenhang mit Fernzugriff und verteilten Arbeitsumgebungen bei.

11.2.2 Klausel 8.1 – Betriebliche Planung und Steuerung: Verlangt die Umsetzung von Kontrollen für Systeme, auf die außerhalb der Unternehmensstandorte zugegriffen wird.

11.2.3 Anhang A Maßnahme 6.7 – Remote-Arbeit: Diese Richtlinie adressiert umfassend die erforderlichen Kontrollen der Informationssicherheit, wenn Personal außerhalb der Unternehmensstandorte arbeitet, einschließlich physischer und logischer Schutzmaßnahmen, Zugriffsgovernance und der Überwachung des Benutzerverhaltens.

11.3 ISO/IEC 27002:2022 – Maßnahme 6

11.3.1 Diese Maßnahme verlangt prozessuale und technische Schutzmaßnahmen für Remote-Arbeit. Sie umfasst Anforderungen an Gerätesicherheit, Zugriffsmethoden, Datenverarbeitung, umgebungsbezogene Schutzmaßnahmen sowie das Management externer Beteiligter – all dies wird durch diese Richtlinie durchgesetzt.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): Wird unmittelbar durch VPN-Kontrollen, Multi-Faktor-Authentifizierung, Sitzungsprotokollierung und rollenbasierte Zugriffsgenehmigung für Remote-Benutzer unterstützt.

11.4.2 AC-2 (Account Management): Regelt die Zugriffsberechtigung, die Zuweisung von Fernzugriffsrechten und die Deaktivierung von Konten.

11.4.3 SC-12 bis SC-13 (Kryptografischer Schutz, Einrichtung kryptografischer Schlüssel): Werden durch die verpflichtende Nutzung von VPNs und Festplattenvollverschlüsselung für Remote-Endpunkte umgesetzt.

11.4.4 MP-5 (Schutz beim Transport von Datenträgern) und PE-18 (Standort von Komponenten des Informationssystems): Die Vorgaben für Remote-Arbeit verlangen Schutz beim Transport und physische Schutzmaßnahmen in externen Umgebungen.

11.4.5 AU-2, AU-6: Protokollierung und Überwachung von Remote-Sitzungen unterstützen Audit- und Incident-Response-Anforderungen.

11.5 DSGVO (2016/679)

11.5.1 Artikel 32 – Sicherheit der Verarbeitung: Diese Richtlinie setzt Sicherheitskontrollen für Fernzugriff, Verschlüsselung und Protokollierung durch, die erforderlich sind, um

personenbezogene Daten zu schützen, auf die remote zugegriffen oder die remote verarbeitet werden.

11.5.2 Artikel 5(1)(f): Stellt sicher, dass personenbezogene Daten, auf die außerhalb des Standorts zugegriffen wird, vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust geschützt sind.

11.5.3 Erwägungsgrund 39: Betont Zugriffsbeschränkung, Integrität und Vertraulichkeit, insbesondere dann, wenn Geräte gesicherte Standorte verlassen.

11.6 EU NIS2-Richtlinie (2022/2555)

11.6.1 Artikel 21(2)(a, b, d): Verlangt, dass Fernzugriff als Teil des IKT-Risikomanagementrahmens einer Organisation abgesichert wird. Diese Richtlinie erfüllt die Anforderung an Sicherheitsmaßnahmen, die Zugriffskontrolle, Datensicherheit und organisatorische Vorgaben für Remote-Umgebungen abdecken.

11.6.2 Artikel 21(3): Fördert Sicherheitsbewusstsein und die Durchsetzung von Richtlinien bei Personal, das außerhalb zentraler Standorte arbeitet.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 – Governance- und internes Kontrollrahmenwerk: Diese Richtlinie unterstützt die Anforderungen an die Steuerung von IKT-Risiken für alle operativen Szenarien, einschließlich hybrider und Remote-Modelle.

11.7.2 Artikel 8 – IKT-Risikomanagementrahmenwerk: Risiken des Fernzugriffs werden über die hier durchgesetzten technischen und organisatorischen Kontrollen identifiziert, gemindert und gesteuert.

11.7.3 Artikel 9 – Vereinbarungen zum Informationsaustausch: Schützt vor Datenabfluss bei Informationen, die innerhalb digitaler Netze zur operationellen Resilienz ausgetauscht werden.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Diese Richtlinie unterstützt die sichere Kontinuität des Geschäftsbetriebs unabhängig vom physischen Arbeitsort.

11.8.2 BAI06 – Managed IT Changes und BAI09 – Managed Assets: Stellen sicher, dass Geräte für Remote-Arbeit nachverfolgt, sicher konfiguriert und als kritische Assets behandelt werden.

11.8.3 APO13 – Managed Security: Fördert ein definiertes Sicherheits-Governance-Modell für Remote-Umgebungen.

11.8.4 MEA03 – Überwachen, Bewerten und Beurteilen der Compliance: Legt fest, dass Aktivitäten der Remote-Arbeit protokolliert, überprüft und auditiert werden müssen.