					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P09S					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**

Ausgerichtet an Standards und Vorschriften, soweit anwendbar

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 6.1, 6.2, 8	
ISO/IEC 27002:2022	Maßnahme 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Artikel 21(2)(b), 21(2)(h)	EU NIS2
EU DORA	Artikel 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
DSGVO	Artikel 32	DSGVO

1. Zweck

1.1 Diese Richtlinie legt Sicherheitsanforderungen für Mitarbeitende und Auftragnehmer fest, die remote arbeiten, einschließlich von zu Hause, in gemeinsam genutzten Arbeitsbereichen oder auf Reisen.

1.2 Sie dient dem Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Geschäftsinformationen, auf die außerhalb von durch das Unternehmen kontrollierten Umgebungen zugegriffen wird.

1.3 Diese Richtlinie gewährleistet die Einhaltung internationaler Standards und reduziert Risiken wie unbefugten Zugriff, Datenverlust und Dienstausfälle.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für sämtliches Personal (Mitarbeitende, Auftragnehmer, Berater und Zeitarbeitskräfte), das bei der Arbeit außerhalb des Unternehmensstandorts auf Unternehmenssysteme, Netzwerke oder Daten zugreift.

2.2 Sie umfasst:

2.2.1 die Nutzung von durch das Unternehmen bereitgestellten sowie privat genutzten Geräten

2.2.2 den Zugriff über VPN, Remote-Desktop oder Cloud-Dienste

2.2.3 den sicheren Umgang mit Informationen außerhalb der Unternehmensräumlichkeiten

2.2.4 Überwachung, Behandlung von Ausnahmen und Durchsetzung

2.3 Sie gilt sowohl für vollständige als auch teilweise Remote-Arbeitsmodelle, einschließlich ad hoc erfolgendem Fernzugriff.

3. Ziele

3.1 Verhinderung des unbefugten Zugriffs auf Unternehmenssysteme oder sensible Daten während der Remote-Arbeit.

3.2 Sicherstellung, dass Geräte und Kommunikationsverbindungen, die außerhalb des Büros genutzt werden, die grundlegenden Sicherheitsanforderungen erfüllen.

3.3 Aufrechterhaltung der Kontrolle über Fernzugriffsberechtigungen und deren Überwachung.

3.4 Bereitstellung klarer Vorgaben für Mitarbeitende und Führungskräfte zu sicheren Arbeitspraktiken bei der Remote-Arbeit.

3.5 Erfüllung der Anforderungen aus ISO, NIS2, DSGVO, DORA und COBIT für ortsunabhängiges und mobiles Arbeiten.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer (GM)

4.1.1 Genehmigt Regelungen zur Remote-Arbeit und überwacht deren Einhaltung.

4.1.2 Eskaliert Informationssicherheitsvorfälle oder wiederholte Nichteinhaltung.

4.1.3 Prüft Ausnahmen und stellt die Nachverfolgung von Vorfällen sicher.

4.2 IT-Support-Dienstleister oder externer IT-Dienstleister

4.2.1 Richtet sicheren Fernzugriff ein (z. B. VPN, Multi-Faktor-Authentifizierung).

4.2.2 Setzt Endgeräteschutz, Verschlüsselung und Gerätekonfigurationen durch.

4.2.3 Unterstützt Benutzer und untersucht technische Sicherheitsvorfälle.

[... 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 der Richtlinie

9.1.1 Der Geschäftsführer (GM) und der IT-Support müssen diese Richtlinie jährlich überprüfen, um sie an technologische, personelle und rechtliche Änderungen anzupassen.

9.2 Auslöser für eine vorzeitige Aktualisierung

9.2.1 Eine unverzügliche Überprüfung ist erforderlich nach:

9.2.1.1 einem wesentlichen Sicherheitsvorfall im Zusammenhang mit Remote-Arbeit

9.2.1.2 Änderungen der Anforderungen aus NIS2, DSGVO oder DORA

9.2.1.3 der Umstellung auf neue Fernzugriffstechnologien (z. B. eine andere VPN-Plattform)

9.3 Versionskontrolle und Archivierung

9.3.1 Alle Versionen dieser Richtlinie müssen:

9.3.1.1 datiert und durch den Geschäftsführer (GM) genehmigt sein

9.3.1.2 mit einer Versionsnummer versehen sein

9.3.1.3 mindestens drei Jahre archiviert werden

9.4 Kommunikation an das Personal

9.4.1 Aktualisierungen dieser Richtlinie sind allen Remote-Benutzern mitzuteilen. Bei jeder wesentlichen Änderung ist eine Bestätigung erforderlich.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie steht mit den folgenden Richtlinien in Verbindung und unterstützt diese:

10.1.1 P2S – Richtlinie zu Rollen und Verantwortlichkeiten in der Governance: Legt fest, wer Fernzugriff autorisiert und überwacht

10.1.2 P4S – Zugriffsrichtlinie: Legt die Einrichtung von sicherem Fernzugriff und Verfahren für den Entzug von Zugriffsrechten fest

10.1.3 P6S – Risikomanagement-Richtlinie: Erfasst und bewertet Risiken im Zusammenhang mit dem Zugriff außerhalb des Unternehmensstandorts

10.1.4 P8S – Richtlinie zur Sensibilisierung und Schulung zur Informationssicherheit: Schult Benutzer zu Risiken der Remote-Arbeit und bewährten Vorgehensweisen

10.1.5 P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle (P30): Regelt die Reaktion auf Fernzugriffsvorfälle wie die Offenlegung von Zugangsdaten oder den Verlust von Geräten

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.1 – Risikobasierte Planung für Fernzugriffsszenarien

11.1.2 Klausel 6.2 – Behandelt Compliance-Verpflichtungen im Personalbereich in mobilen beziehungsweise Remote-Kontexten

11.1.3 Klausel 8.1 – Operative Planung und Steuerung von Remote-Prozessen

11.2 ISO/IEC 27002

11.2.1 Maßnahme 6.7 – Gibt praxisorientierte Anleitung zur Sicherheit für ortsunabhängiges und mobiles Arbeiten

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Fernzugriffskontrolle, Sitzungsschutz und Sicherheitsüberwachung

11.3.2 AC-2 – Kontenverwaltung für Benutzer außerhalb des Unternehmensstandorts

11.4 DSGVO

11.4.1 Artikel 32 – Verlangt Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, auch in Remote-Umgebungen

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(b) – Verlangt die sichere Nutzung von Netz- und Informationssystemen

11.5.2 Artikel 21(2)(h) – Fordert personenbezogene Sicherheitsmaßnahmen einschließlich Kontrollen außerhalb des Unternehmensstandorts

11.6 EU DORA

11.6.1 Artikel 9 – Verlangt von Finanzunternehmen die Aufrechterhaltung der IKT-Resilienz in allen Betriebsmodi, einschließlich Fernzugriff

11.7 COBIT 2019

11.7.1 DSS05 – Sicherheitsdienste verwalten: Umfasst Endgeräteschutz und sichere Arbeitspraktiken für Remote-Arbeit

11.7.2 APO13 – Managed Security: Stellt die sichere Bereitstellung und Risikoaufsicht für mobilen beziehungsweise Fernzugriff sicher