					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P09S					Dokumenttitel: **Politik for fjernarbejde**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler, hvor det er relevant

Standard/regulering	Klausul/artikel	Bemærkning
ISO/IEC 27001:2022	Punkt 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrol 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Artikel 21, stk. 2, litra b og h	EU NIS2
EU DORA	Artikel 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
GDPR	Artikel 32	GDPR

1. Formål

1.1 Denne politik fastsætter sikkerhedskrav for medarbejdere og kontraktansatte, der arbejder eksternt, herunder fra hjemmet, fælles arbejdspladser eller under rejser.

1.2 Formålet er at beskytte fortroligheden, integriteten og tilgængeligheden af forretningsoplysninger, der tilgås uden for virksomhedens kontrollerede miljøer.

1.3 Denne politik skal sikre efterlevelse af relevante internationale standarder og reducere risici såsom uautoriseret adgang, datatab og driftsforstyrrelser.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, herunder ansatte, kontraktansatte, konsulenter og midlertidigt ansatte, der tilgår virksomhedens systemer, netværk eller data under arbejde uden for virksomhedens lokationer.

2.2 Den omfatter:

2.2.1 Brug af virksomhedsudstedte og private enheder

2.2.2 Adgang via VPN, fjernskrivebord eller cloudtjenester

2.2.3 Sikker håndtering af oplysninger uden for virksomhedens lokationer

2.2.4 Overvågning, undtagelseshåndtering og håndhævelse

2.3 Den gælder for både faste og deltidsbaserede ordninger for fjernarbejde, herunder ad hoc-fjernadgang.

3. Mål

3.1 Forebygge uautoriseret adgang til virksomhedens systemer og følsomme data under fjernarbejde.

3.2 Sikre, at enheder og kommunikationsforbindelser, der anvendes uden for kontoret, opfylder de fastsatte sikkerhedskrav.

3.3 Opretholde kontrol med rettigheder til fjernadgang og tilhørende overvågning.

3.4 Give klare retningslinjer til medarbejdere og ledere om sikker arbejdspraksis ved fjernarbejde.

3.5 Opfylde relevante krav og forventninger i ISO, NIS2, GDPR, DORA og COBIT vedrørende fjernarbejde og mobilt arbejde.

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender ordninger for fjernarbejde og følger op på efterlevelse.

4.1.2 Eskalerer sikkerhedshændelser eller gentagen manglende efterlevelse.

4.1.3 Gennemgår undtagelser og sikrer opfølgning på hændelser.

4.2 IT-support eller ekstern IT-leverandør

4.2.1 Etablerer sikker fjernadgang, herunder VPN og MFA.

4.2.2 Håndhæver endepunktssikkerhed, kryptering og enhedskonfigurationer.

4.2.3 Understøtter brugere og undersøger tekniske sikkerhedshændelser og -problemer.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Årlig gennemgang af politikken

9.1.1 Direktøren og IT-support skal gennemgå denne politik årligt for at sikre, at den er afstemt med ændringer i teknologi, arbejdsformer og lovgivning.

9.2 Udløsende forhold for tidlig opdatering

9.2.1 Øjeblikkelig gennemgang kræves efter:

9.2.1.1 En større sikkerhedshændelse relateret til fjernarbejde

9.2.1.2 Ændringer i krav efter NIS2, GDPR eller DORA

9.2.1.3 Overgang til ny teknologi til fjernadgang, herunder en anden VPN-platform

9.3 Versionsstyring og arkivering

9.3.1 Alle versioner af denne politik skal være:

9.3.1.1 Dateret og godkendt af direktøren

9.3.1.2 Forsynet med versionsnummer

9.3.1.3 Arkiveret i mindst tre år

9.4 Kommunikation til medarbejdere

9.4.1 Opdateringer til politikken skal kommunikeres til alle fjernbrugere. Bekræftelse kræves ved væsentlige ændringer.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er forbundet med og understøtter følgende:

10.1.1 P2S – Politik for roller og ansvar i styringen: Definerer, hvem der godkender og fører tilsyn med fjernadgang

10.1.2 P4S – Politik for adgangskontrol: Fastlægger procedurer for sikker etablering og tilbagekaldelse af fjernadgang

10.1.3 P6S – Politik for risikostyring: Registrerer og vurderer risici forbundet med adgang uden for virksomhedens lokationer

10.1.4 P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Uddanner brugere i risici ved fjernarbejde og god praksis

10.1.5 P30S – Politik for hændelseshåndtering: Regulerer håndtering af hændelser ved fjernadgang, såsom lækage af legitimationsoplysninger eller tab af enheder

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – Risikobaseret planlægning for scenarier med fjernadgang

11.1.2 Punkt 6.2 – Omhandler HR-ansvar i mobile og eksterne arbejdskontekster

11.1.3 Punkt 8.1 – Operationel planlægning og styring af fjernrelaterede processer

11.2 ISO/IEC 27002

11.2.1 Kontrol 6.7 – Giver praktisk vejledning om sikkerhed ved fjernarbejde og mobilt arbejde

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Kontrol med fjernadgang, sessionsbeskyttelse og sikkerhedsovervågning

11.3.2 AC-2 – Kontrol med brugerkonti for brugere uden for virksomhedens lokationer

11.4 GDPR

11.4.1 Artikel 32 – Kræver passende sikkerhedsforanstaltninger, herunder i fjernmiljøer

11.5 NIS2-direktivet

11.5.1 Artikel 21, stk. 2, litra b – Kræver sikker anvendelse af net- og informationssystemer

11.5.2 Artikel 21, stk. 2, litra h – Forudsætter HR-relaterede sikkerhedsforanstaltninger, herunder kontroller uden for virksomhedens lokationer

11.6 EU DORA

11.6.1 Artikel 9 – Kræver, at finansielle enheder opretholder IKT-robusthed på tværs af alle driftsformer, herunder fjernadgang

11.7 COBIT 2019

11.7.1 DSS05 – Manage Security Services: Omfatter beskyttelse af endepunkter og sikre arbejdspraksisser ved fjernarbejde

11.7.2 APO13 – Managed Security: Sikrer sikker etablering og risikotilsyn for mobil og fjernadgang