					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P09					Dokumenttitel: **Fjernarbejdspolitik**							
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**

1. Formål

1.1 Denne politik fastlægger de obligatoriske krav til sikker udførelse af fjernarbejde, herunder brug af organisationens informationssystemer, adgang til data og udførelse af arbejdsopgaver uden for organisationens lokationer.

1.2 Den sikrer fortrolighed, integritet og tilgængelighed (CIA) for informationsaktiver, der tilgås eksternt, og etablerer kontroller til at reducere risici forbundet med distribuerede arbejdsmiljøer.

1.3 Politikken opfylder ISO/IEC 27001:2022 Annex A Control 6.7 ved at implementere tekniske kontroller og proceduremæssige sikkerhedsforanstaltninger tilpasset forholdene ved fjernarbejde.

2. Omfang

2.1 Denne politik gælder for alt personale, der er godkendt til at arbejde eksternt, herunder:

2.1.1 Medarbejdere (fuldtid, deltid, kontraktansatte)

2.1.2 Eksterne tjenesteudbydere, konsulenter og leverandører

2.1.3 Midlertidigt ansatte og projektansatte med godkendt fjernadgang (VPN, administration af mobile enheder)

2.2 Den omfatter:

2.2.1 Adgang til organisationens informationssystemer via VPN eller godkendte værktøjer til fjernadgang

2.2.2 Håndtering af følsomme og regulerede oplysninger uden for sikre faciliteter

2.2.3 Brug af organisationsejet udstyr eller personligt ejede enheder under en godkendt BYOD-ordning

2.2.4 Beskyttelse af fysisk og logisk adgang i fjernmiljøer

2.3 Politikken gælder på tværs af alle geografier og tidszoner, hvor organisationen tillader fjernarbejde, uanset om det er fast, ad hoc eller i forbindelse med hændelser relateret til forretningskontinuitet.

3. Mål

3.1 At sikre, at kun autoriserede personer kan opnå fjernadgang til interne systemer og oplysninger.

3.2 At håndhæve kryptering, multifaktorgodkendelse (MFA) og endepunktssikkerhed på tværs af alle fjernadgangsveje.

3.3 At opretholde et sikkerhedsniveau mod trusler som phishing, malware, dataeksfiltrering og uautoriseret eksponering af systemer.

3.4 At styre, hvordan følsomme data overføres, opbevares eller udskrives i miljøer uden for organisationens lokationer.

3.5 At indarbejde fysiske sikkerhedsforanstaltninger, der reducerer synlighed og uautoriseret observation under fjernsessioner.

3.6 At overholde internationale regulatoriske krav vedrørende fjernadgang til data, herunder GDPR, NIS2 og DORA.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og sikrer, at de nødvendige ressourcer stilles til rådighed, og at politikken integreres i HR-, IT- og sikkerhedsdriften.

4.1.2 Godkender organisationens kriterier for berettigelse til fjernarbejde og anvendelsen heraf i forretningsenhederne.

4.2 CISO/ISMS-ansvarlig

4.2.1 Er ansvarlig for politikken, vedligeholder den og sikrer, at den er afstemt med risikobilledet og regulatoriske krav.

4.2.2 Definerer sikkerhedskontroller for fjernadgang (f.eks. kryptering, endepunktsbeskyttelse og sessions-timeout).

4.2.3 Godkender håndtering af undtagelser og overvåger kontroludførelsen.

[... 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 Frekvens for gennemgang

9.1.1 Denne politik skal gennemgås årligt eller hyppigere ved:

9.1.1.1 Indførelse af nye teknologier til fjernadgang

9.1.1.2 Væsentlig udvidelse af fjernarbejde (f.eks. initiativer for hybride arbejdsformer)

9.1.1.3 Fremkomst af nye trusler, sårbarheder eller hændelser knyttet til fjernmiljøer

9.1.1.4 Ændringer i relevante juridiske eller regulatoriske rammer

9.2 Ejerskab og proces for gennemgang

9.2.1 Politikejeren er CISO. Gennemgangen skal koordineres med:

9.2.1.1 IT-drift og arkitektur

9.2.1.2 HR og Facility Management (for driftsmæssige konsekvenser og konsekvenser for arbejdsområder)

9.2.1.3 Databeskyttelsesrådgiveren (for databeskyttelse og grænseoverskridende datakontroller)

9.2.2 Opdateringer af politikken skal:

9.2.2.1 Godkendes af informationssikkerhedsstyregruppen (ISSC)

9.2.2.2 Kommunikeres til alle berørte medarbejdere og kontrahenter

9.2.2.3 Integreres i materialer til onboarding og genopfriskningstræning

9.3 Dokumentstyring og distribution

9.3.1 Politikken skal indeholde versionsstyring, ikrafttrædelsesdato og ændringshistorik.

9.3.2 Erstattede versioner skal opbevares i henhold til politikken for dokumentstyring (P14).

9.3.3 Reviderede versioner skal udløse obligatorisk fornyet bekræftelse for brugere, der er berettiget til fjernarbejde.

10. Relaterede politikker og sammenhænge

10.1 Denne politik fungerer i sammenhæng med:

10.1.1 P1 – Informationssikkerhedspolitik: Etablerer baseline for sikker håndtering af aktiver, som gælder for alle arbejdsmiljøer, herunder fjernarbejde.

10.1.2 P3 – Politik for acceptabel brug: Regulerer korrekt brug af organisationens enheder og systemer under fjernarbejdssessioner.

10.1.3 P4 – Politik for adgangskontrol: Sikrer, at privilegier til fjernadgang følger princippet om mindst privilegium og korrekte autentificeringsmekanismer.

10.1.4 P6 – Politik for risikostyring: Definerer, hvordan risici ved fjernarbejde identificeres, behandles og overvåges inden for ISMS.

10.1.5 P12 – Politik for aktivstyring: Kræver aktivfortegnelse og konfigurationsstyring for alle enheder, der anvendes til fjernarbejde.

10.1.6 P22 – Lognings- og overvågningspolitik: Sikrer, at fjernsessioner overvåges, auditeres og opbevares i henhold til gældende efterlevelseskrav.

10.1.7 P14 – Politik for dataopbevaring og bortskaffelse: Definerer regler for datahåndtering, der er relevante for fjernarbejde, herunder flytbare medier og bortskaffelse af enheder.

10.2 Disse politikker sikrer samlet, at fjernarbejde er sikkert, i overensstemmelse med kravene og kan håndhæves på tværs af alle funktioner og geografier.

11. Referencestandarder og rammeværk

11.1 Denne politik er afstemt med internationalt anerkendte rammeværk for sikkerhed, databeskyttelse og styring af IKT-risici for at sikre sikker, sporbar og konsistent praksis for fjernarbejde.

11.2 ISO/IEC 27001

11.2.1 Clause 6.1.3 – planlægning af risikobehandling: Denne politik bidrager til behandlingen af risici forbundet med fjernadgang og distribuerede arbejdsmiljøer.

11.2.2 Clause 8.1 – driftsplanlægning og styring: Kræver implementering af kontroller for systemer, der tilgås uden for organisationens lokationer.

11.2.3 Annex A Control 6.7 – fjernarbejde: Denne politik adresserer fuldt ud de krævede informationssikkerhedskontroller, når personale arbejder uden for organisationens lokationer, herunder beskyttelse af fysisk og logisk adgang, adgangsstyring og overvågning af brugeradfærd.

11.3 ISO/IEC 27002:2022 – Control 6

11.3.1 Denne kontrol kræver proceduremæssige sikkerhedsforanstaltninger og tekniske kontroller for fjernarbejde. Den omfatter krav til enhedssikkerhed, adgangsmetoder, datahåndtering, miljømæssige sikkerhedsforanstaltninger og styring af tredjeparter, som alle håndhæves gennem denne politik.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): Understøttes direkte via VPN-kontroller, MFA, sessionslogning og rollebaseret godkendelse af adgang for fjernbrugere.

11.4.2 AC-2 (Account Management): Regulerer adgangsberettigelse, tildeling af fjernprivilegier og deaktivering af konti.

11.4.3 SC-12 til SC-13 (Cryptographic Protection, Cryptographic Key Establishment): Implementeres gennem obligatorisk brug af VPN og fulddiskkryptering for eksterne endepunkter.

11.4.4 MP-5 (Media Transport Protection) og PE-18 (Location of Information System Components): Retningslinjerne for fjernarbejde kræver beskyttelse under transport og fysiske sikkerhedsforanstaltninger i miljøer uden for organisationens lokationer.

11.4.5 AU-2, AU-6: Logning og overvågning af fjernsessioner understøtter krav til revision og hændelsesrespons.

11.5 EU GDPR (2016/679)

11.5.1 Article 32 – behandlingssikkerhed: Denne politik håndhæver sikkerhedskontroller for fjernadgang, kryptering og logning, som er nødvendige for at beskytte personoplysninger, der tilgås eller behandles eksternt.

11.5.2 Article 5(1)(f): Sikrer, at personoplysninger, der tilgås uden for organisationens lokationer, er beskyttet mod uautoriseret eller ulovlig behandling samt hændeligt tab.

11.5.3 Recital 39: Fremhæver begrænsning af adgang, integritet og fortrolighed, hvilket er særligt relevant, når enheder forlader sikre lokationer.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Article 21(2)(a, b, d): Kræver, at fjernadgang sikres som en del af organisationens ramme for styring af IKT-risici. Denne politik opfylder kravet om sikkerhedsforanstaltninger, der dækker adgangsstyring, datasikkerhed og organisatoriske politikker for fjernmiljøer.

11.6.2 Article 21(3): Fremmer sikkerhedsbevidsthed og håndhævelse af politikker blandt medarbejdere, der arbejder uden for centrale lokationer.

11.7 EU DORA (2022/2554)

11.7.1 Article 5 – Governance and Internal Control Framework: Denne politik understøtter kravene til styring af IKT-risici i alle driftsmæssige scenarier, herunder hybride og eksterne arbejdsmodeller.

11.7.2 Article 8 – ICT Risk Management Framework: Risici ved fjernadgang identificeres, afbødes og styres gennem tekniske og organisatoriske kontroller, som håndhæves her.

11.7.3 Article 9 – Information Sharing Arrangements: Beskytter mod fjernrelateret lækage af oplysninger, der deles i ordninger for digital operationel robusthed.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Denne politik understøtter sikker videreførelse af forretningsdriften uanset fysisk placering.

11.8.2 BAI06 – Managed IT Changes og BAI09 – Managed Assets: Sikrer, at enheder til fjernarbejde spores, konfigureres sikkert og håndteres som kritiske aktiver.

11.8.3 APO13 – Managed Security: Understøtter en defineret styringsramme for sikkerhed i fjernmiljøer.

11.8.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Fastlægger, at aktiviteter ved fjernarbejde skal logges, gennemgås og auditeres.