					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P09S					Documenttitel: **Beleid inzake werken op afstand**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 6.1, 6.2, 8	
ISO/IEC 27002:2022	Beheersmaatregel 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Artikelen 21(2)(b), 21(2)(h)	EU NIS2
EU DORA	Artikel 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EU AVG	Artikel 32	EU AVG

1. Doel

1.1 Dit beleid stelt beveiligingseisen vast voor medewerkers en opdrachtnemers die op afstand werken, waaronder vanuit huis, gedeelde werkruimten of tijdens reizen.

1.2 Dit beleid heeft tot doel de vertrouwelijkheid, integriteit en beschikbaarheid (CIA) te beschermen van bedrijfsinformatie die wordt geraadpleegd buiten door de organisatie beheerde omgevingen.

1.3 Dit beleid waarborgt naleving van internationale normen en beperkt risico's zoals ongeautoriseerde toegang, gegevensverlies en verstoring van de dienstverlening.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle medewerkers (werknemers, opdrachtnemers, consultants en tijdelijke krachten) die toegang hebben tot bedrijfssystemen, netwerken of gegevens terwijl zij buiten de bedrijfslocatie werken.

2.2 Dit beleid omvat:

2.2.1 Het gebruik van door de organisatie verstrekte en privéapparaten

2.2.2 Toegang via VPN, remote desktop of clouddiensten

2.2.3 Veilige verwerking van informatie buiten de bedrijfslocaties

2.2.4 Monitoring, uitzonderingsbeheer en handhaving

2.3 Dit beleid is van toepassing op zowel structurele als gedeeltelijke regelingen voor werken op afstand, met inbegrip van ad-hoctoegang op afstand.

3. Doelstellingen

3.1 Voorkomen van ongeautoriseerde toegang tot bedrijfssystemen of gevoelige gegevens tijdens het werken op afstand.

3.2 Waarborgen dat apparaten en communicatieverbindingen die buiten kantoor worden gebruikt voldoen aan de beveiligingsbaseline.

3.3 Behoud van controle op toegangsrechten voor toegang op afstand en op monitoring.

3.4 Bieden van duidelijke richtlijnen aan medewerkers en leidinggevenden voor veilige werkwijzen bij werken op afstand.

3.5 Voldoen aan de verwachtingen van ISO, NIS2, AVG, DORA en COBIT ten aanzien van werken op afstand en mobiel werken.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Keurt regelingen voor werken op afstand goed en ziet toe op naleving.

4.1.2 Escaleert beveiligingsincidenten of herhaalde niet-naleving.

4.1.3 Beoordeelt uitzonderingen en waarborgt opvolging van incidenten.

4.2 IT-ondersteuning of externe IT-dienstverlener

4.2.1 Richt veilige toegang op afstand in (bijvoorbeeld VPN, multifactorauthenticatie).

4.2.2 Dwingt endpointbeveiliging, versleuteling en apparaatconfiguraties af.

4.2.3 Ondersteunt gebruikers en onderzoekt technische beveiligingsincidenten.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Vereisten voor beoordeling en actualisatie

9.1 Jaarlijkse beleidsbeoordeling

9.1.1 De algemeen directeur (GM) en IT-ondersteuning moeten dit beleid jaarlijks beoordelen om het af te stemmen op wijzigingen in technologie, personeelsbestand en wet- en regelgeving.

9.2 Triggers voor vervroegde actualisatie

9.2.1 Onmiddellijke beoordeling is vereist na:

9.2.1.1 Een ernstig beveiligingsincident met betrekking tot werken op afstand

9.2.1.2 Wijzigingen in vereisten van NIS2, AVG of DORA

9.2.1.3 Overgang naar nieuwe technologie voor toegang op afstand (bijvoorbeeld een ander VPN-platform)

9.3 Versiebeheer en archivering

9.3.1 Alle versies van dit beleid moeten:

9.3.1.1 Zijn gedateerd en goedgekeurd door de algemeen directeur (GM)

9.3.1.2 Zijn voorzien van een versienummer

9.3.1.3 Ten minste drie jaar worden gearchiveerd

9.4 Communicatie aan medewerkers

9.4.1 Beleidsactualisaties moeten aan alle gebruikers op afstand worden gecommuniceerd. Voor elke significante wijziging is kennisneming van het beleid vereist.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid houdt verband met en ondersteunt het volgende:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: Definieert wie toegang op afstand autoriseert en hierop toezicht houdt

10.1.2 P4S – Beleid inzake toegangsbeveiliging: Stelt procedures vast voor veilige inrichting en intrekking van toegang op afstand

10.1.3 P6S – Risicobeheerbeleid: Volgt en beoordeelt risico's die verband houden met toegang buiten de bedrijfslocatie

10.1.4 P8S – Beleid inzake bewustwording en opleiding op het gebied van informatiebeveiliging: Leidt gebruikers op over risico's van werken op afstand en best practices

10.1.5 P30S – Incidentresponsbeleid: Regelt de respons op incidenten met toegang op afstand, zoals het lekken van inloggegevens of verlies van apparaten

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1 – Risicogebaseerde planning voor scenario's met toegang op afstand

11.1.2 Clausule 6.2 – Behandelt HR-verantwoordelijkheden in mobiele contexten en contexten van werken op afstand

11.1.3 Clausule 8.1 – Operationele planning en beheersing van processen op afstand

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 6.7 – Geeft praktische richtlijnen voor de beveiliging van werken op afstand en mobiel werken

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Beheersing van toegang op afstand, sessiebeveiliging en beveiligingsmonitoring

11.3.2 AC-2 – Accountbeheer voor gebruikers buiten de bedrijfslocatie

11.4 EU AVG

11.4.1 Artikel 32 – Vereist gegevensbescherming by design en by default, ook in contexten van werken op afstand

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(b) – Vereist veilig gebruik van netwerk- en informatiesystemen

11.5.2 Artikel 21(2)(h) – Vereist HR-gerelateerde beveiligingsmaatregelen, waaronder beheersmaatregelen buiten de bedrijfslocatie

11.6 EU DORA

11.6.1 Artikel 9 – Vereist dat financiële entiteiten ICT-veerkracht handhaven in alle operationele modi, waaronder toegang op afstand

11.7 COBIT 2019

11.7.1 DSS05 – Beheer van beveiligingsdiensten: Omvat endpointbescherming en veilige werkwijzen voor werken op afstand

11.7.2 APO13 – Beheerde beveiliging: Waarborgt veilige toegangsverlening en risicotoezicht voor mobiele toegang en toegang op afstand