					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P09					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**

1. Doel

1.1 Dit beleid definieert de verplichte eisen voor het veilig uitvoeren van werkzaamheden op afstand, waaronder het gebruik van informatiesystemen van de organisatie, toegang tot gegevens en de uitvoering van werkzaamheden buiten de bedrijfsruimten.

1.2 Het waarborgt de vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van informatieactiva die op afstand worden benaderd en stelt beheersmaatregelen vast om risico's in gedistribueerde werkomgevingen te beperken.

1.3 Dit beleid geeft invulling aan ISO/IEC 27001:2022 Bijlage A, beheersmaatregel 6.7, door technische en procedurele beveiligingsmaatregelen te implementeren die zijn afgestemd op werken op afstand.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle medewerkers die bevoegd zijn om op afstand te werken, waaronder:

2.1.1 Werknemers (voltijd, deeltijd, op contractbasis)

2.1.2 Externe dienstverleners, consultants en leveranciers

2.1.3 Tijdelijke krachten en projectmedewerkers met goedgekeurde externe toegang (VPN, mobielapparaatbeheer)

2.2 Dit beleid omvat:

2.2.1 Toegang tot informatiesystemen van de organisatie via VPN of goedgekeurde voorzieningen voor externe toegang

2.2.2 Verwerking van gevoelige en gereguleerde informatie buiten beveiligde gebieden

2.2.3 Gebruik van apparatuur van de organisatie of Bring Your Own Device (BYOD)

2.2.4 Fysieke beheersmaatregelen en logische toegangsbeveiliging in omgevingen voor werken op afstand

2.3 Dit beleid geldt voor alle geografische locaties en tijdzones waar de organisatie werken op afstand toestaat, ongeacht of dit structureel, ad hoc of in het kader van bedrijfscontinuïteit plaatsvindt.

3. Doelstellingen

3.1 Waarborgen dat uitsluitend geautoriseerde personen op afstand toegang hebben tot interne systemen en informatie.

3.2 Afdwingen van encryptie, multifactorauthenticatie en endpointbeveiliging voor alle vormen van toegang op afstand.

3.3 Handhaven van een passende risicopositie op het gebied van informatiebeveiliging ten aanzien van dreigingen zoals phishing, malware, data-exfiltratie en ongeautoriseerde blootstelling van systemen.

3.4 Vastleggen hoe gevoelige gegevens buiten de locatie mogen worden verzonden, opgeslagen of afgedrukt.

3.5 Verankeren van fysieke beheersmaatregelen die zichtbaarheid en ongeautoriseerde observatie tijdens sessies op afstand beperken.

3.6 Voldoen aan internationale wettelijke en regelgevende vereisten voor toegang op afstand tot gegevens, waaronder de AVG, NIS2 en DORA.

4. Rollen en verantwoordelijkheden

4.1 Het topmanagement

4.1.1 Keurt dit beleid goed en zorgt ervoor dat hiervoor voldoende middelen beschikbaar zijn en dat het wordt geïntegreerd in HR-processen, IT-operaties en beveiligingsoperaties.

4.1.2 Autoriseert de criteria voor geschiktheid voor werken op afstand en de toepasbaarheid per bedrijfseenheid.

4.2 CISO / ISMS-manager

4.2.1 Is eigenaar van dit beleid, houdt het actueel en waarborgt afstemming op de risicopositie en nalevingsverplichtingen.

4.2.2 Definieert beveiligingsmaatregelen voor toegang op afstand, zoals encryptie, endpointbeveiliging en sessietime-outs.

4.2.3 Keurt uitzonderingsbeheer goed en bewaakt de doeltreffendheid van beheersmaatregelen.

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

9. Eisen voor herziening en actualisering

9.1 Beoordelingsfrequentie

9.1.1 Dit beleid moet jaarlijks worden beoordeeld, of vaker bij:

9.1.1.1 Introductie van nieuwe technologieën voor externe toegang

9.1.1.2 Aanzienlijke uitbreiding van werken op afstand, zoals initiatieven voor hybride werkmodellen

9.1.1.3 Ontstaan van nieuwe dreigingen, kwetsbaarheden of incidenten die verband houden met omgevingen voor werken op afstand

9.1.1.4 Wijzigingen in relevante wettelijke of regelgevende kaders

9.2 Eigenaarschap en beoordelingsproces

9.2.1 De eigenaar van dit beleid is de CISO. De beoordeling moet worden gecoördineerd met:

9.2.1.1 IT-operaties en architectuur

9.2.1.2 HR, Facilitair en assetmanagement voor operationele gevolgen en gevolgen voor de werkplek

9.2.1.3 De functionaris voor gegevensbescherming voor privacy en beheersmaatregelen inzake grensoverschrijdende gegevens

9.2.2 Actualisaties van het beleid moeten:

9.2.2.1 Worden goedgekeurd door de ISMS-stuurgroep

9.2.2.2 Worden gecommuniceerd aan alle betrokken medewerkers en contractanten

9.2.2.3 Worden geïntegreerd in onboardingmateriaal en materiaal voor opfristraining

9.3 Documentbeheersing en distributie

9.3.1 Het beleid moet versiebeheer, ingangsdatum en versiehistorie bevatten.

9.3.2 Vervangen versies moeten worden bewaard conform het beleid voor documentbeheer (P14).

9.3.3 Herziene versies moeten een verplichte hernieuwde kennisname activeren voor gebruikers die in aanmerking komen voor werken op afstand.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid hangt samen met:

10.1.1 P1 – Informatiebeveiligingsbeleid: Stelt de baseline vast voor veilige omgang met bedrijfsmiddelen, van toepassing op alle werkomgevingen, waaronder werken op afstand.

10.1.2 P3 – Beleid inzake aanvaardbaar gebruik: Regelt het passende gebruik van apparaten en systemen van de organisatie tijdens sessies voor werken op afstand.

10.1.3 P4 – Beleid inzake toegangscontrole: Borgt dat bevoegdheden voor externe toegang in lijn zijn met het least-privilegeprincipe en passende authenticatiemechanismen.

10.1.4 P6 – Risicobeheerbeleid: Bepaalt hoe risico's met betrekking tot werken op afstand binnen het ISMS worden geïdentificeerd, behandeld en bewaakt.

10.1.5 P12 – Assetmanagementbeleid: Verplicht inventarisatie en configuratiebeheer voor alle apparaten die op afstand worden gebruikt.

10.1.6 P22 – Logging- en monitoringbeleid: Borgt dat sessies op afstand worden gemonitord, geaudit en bewaard conform nalevingseisen.

10.1.7 P14 – Beleid inzake gegevensbewaring en afvoer: Definieert regels voor gegevensverwerking die relevant zijn voor werken op afstand, waaronder verwijderbare media en afvoer van apparaten.

10.2 Deze beleidslijnen waarborgen gezamenlijk dat werken op afstand veilig, compliant en afdwingbaar is binnen alle functies en geografische gebieden.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende raamwerken voor beveiliging, gegevensbescherming en ICT-risicobeheer om veilige, traceerbare en conforme werkwijzen voor werken op afstand te waarborgen.

11.2 ISO/IEC 27001

11.2.1 Clausule 6.1.3 – Planning van risicobehandeling: Dit beleid draagt bij aan de behandeling van risico's die samenhangen met externe toegang en gedistribueerde werkomgevingen.

11.2.2 Clausule 8.1 – Operationele planning en beheersing: Vereist de implementatie van beheersmaatregelen voor systemen die buiten de bedrijfsruimten worden benaderd.

11.2.3 Bijlage A, beheersmaatregel 6.7 – Werken op afstand: Dit beleid geeft volledig invulling aan de vereiste beheersmaatregelen voor informatiebeveiliging wanneer personeel buiten de bedrijfsruimten werkt, waaronder fysieke beheersmaatregelen, logische toegang, toegangsgovernance en monitoring van gebruikersgedrag.

11.3 ISO/IEC 27002:2022 – Beheersmaatregel 6

11.3.1 Deze beheersmaatregel vereist procedurele en technische beveiligingsmaatregelen voor werken op afstand. Dit omvat eisen voor apparaatbeveiliging, toegangsmethoden, gegevensverwerking, omgevingsbeheersmaatregelen en het beheer van externe partijen; al deze vereisten worden via dit beleid afgedwongen.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): Rechtstreeks ondersteund via VPN-beheersmaatregelen, MFA, sessielogging en rolgebaseerde autorisatie van externe toegang voor gebruikers op afstand.

11.4.2 AC-2 (Account Management): Beheerst geschiktheid voor toegang, toewijzing van rechten voor externe toegang en deactivering van accounts.

11.4.3 SC-12 tot SC-13 (Cryptographic Protection, Cryptographic Key Establishment): Geïmplementeerd door het verplichte gebruik van VPN's en volledige schijfversleuteling voor externe endpoints.

11.4.4 MP-5 (Media Transport Protection) en PE-18 (Location of Information System Components): Richtlijnen voor werken op afstand verplichten transportbeveiliging en fysieke beveiligingsmaatregelen in omgevingen buiten de bedrijfslocatie.

11.4.5 AU-2, AU-6: Logging en monitoring van sessies op afstand ondersteunen vereisten voor audits en incidentrespons.

11.5 EU AVG (2016/679)

11.5.1 Artikel 32 – Beveiliging van de verwerking: Dit beleid dwingt beveiligingsmaatregelen voor externe toegang, encryptie en logging af die nodig zijn om persoonsgegevens die op afstand worden benaderd of verwerkt te beveiligen.

11.5.2 Artikel 5(1)(f): Waarborgt dat persoonsgegevens die buiten de locatie worden benaderd worden beschermd tegen ongeautoriseerde of onrechtmatige verwerking en tegen onopzettelijk verlies.

11.5.3 Overweging 39: Benadrukt beperking van toegang, integriteit en vertrouwelijkheid, in het bijzonder wanneer apparaten beveiligde ruimten verlaten.

11.6 EU NIS2-richtlijn (2022/2555)

11.6.1 Artikel 21(2)(a, b, d): Vereist dat externe toegang wordt beveiligd als onderdeel van het ICT-risicobeheerkader van een organisatie. Dit beleid geeft invulling aan de vereiste beveiligingsmaatregelen voor toegangscontrole, gegevensbeveiliging en organisatorische beleidslijnen voor omgevingen voor werken op afstand.

11.6.2 Artikel 21(3): Stimuleert beveiligingsbewustzijn en handhaving van beleid onder medewerkers die buiten centrale locaties werken.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 – Governance- en internebeheersingskader: Dit beleid ondersteunt verwachtingen ten aanzien van ICT-risicobeheersing voor alle operationele scenario's, waaronder hybride en externe werkmodellen.

11.7.2 Artikel 8 – ICT-risicobeheerkader: Risico's van externe toegang worden geïdentificeerd, beperkt en beheerst via de hier afgedwongen technische en organisatorische beheersmaatregelen.

11.7.3 Artikel 9 – Regelingen voor het delen van informatie: Beschermt tegen het uitlekken van informatie op afstand binnen netwerken voor digitale operationele weerbaarheid.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Dit beleid ondersteunt de veilige continuïteit van bedrijfsactiviteiten ongeacht de fysieke locatie.

11.8.2 BAI06 – Managed IT Changes en BAI09 – Managed Assets: Waarborgen dat apparaten voor werken op afstand worden gevolgd, veilig worden geconfigureerd en als kritieke activa worden behandeld.

11.8.3 APO13 – Managed Security: Bevordert een gedefinieerd kader voor informatiebeveiligingsgovernance voor omgevingen voor werken op afstand.

11.8.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Stelt vast dat activiteiten inzake werken op afstand moeten worden gelogd, beoordeeld en geaudit.