					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P09					Dokumenttitel: **Policy för distansarbete**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

1. Syfte

1.1 Denna policy fastställer obligatoriska krav för att bedriva distansarbete på ett säkert sätt, inklusive användning av organisationens system, åtkomst till data och utförande av arbetsuppgifter utanför organisationens lokaler.

1.2 Den säkerställer konfidentialitet, riktighet och tillgänglighet för informationstillgångar som nås på distans samt fastställer kontroller för att begränsa risker kopplade till distribuerade arbetsmiljöer.

1.3 Policyn uppfyller ISO/IEC 27001:2022 bilaga A, kontroll 6.7, genom att införa tekniska och administrativa skyddsåtgärder anpassade för distansarbete.

2. Omfattning

2.1 Denna policy gäller för all personal som har behörighet att arbeta på distans, inklusive:

2.1.1 anställda (heltid, deltid, kontrakterade)

2.1.2 externa tjänsteleverantörer, konsulter och leverantörer

2.1.3 tillfälligt anställda och projektanställda med godkänd fjärråtkomst

2.2 Den omfattar:

2.2.1 åtkomst till organisationens system via VPN eller godkända fjärråtkomstverktyg

2.2.2 hantering av känslig och reglerad information utanför säkra områden

2.2.3 användning av utrustning som ägs av organisationen eller privata enheter (BYOD)

2.2.4 fysiska och logiska skydd i distansarbetsmiljöer

2.3 Policyn gäller i samtliga geografier och tidszoner där organisationen tillåter distansarbete, oavsett om det sker regelbundet, ad hoc eller inom ramen för verksamhetskontinuitet.

3. Mål

3.1 Säkerställa att endast behöriga personer kan få fjärråtkomst till interna system och information.

3.2 Säkerställa användning av kryptering, flerfaktorsautentisering (MFA) och slutpunktsskydd i samtliga fjärråtkomstvägar.

3.3 Upprätthålla ett skydd mot hot såsom phishing, skadlig kod, dataexfiltration och otillåten exponering av system.

3.4 Styra hur känsliga data överförs, lagras eller skrivs ut i miljöer utanför organisationens lokaler.

3.5 Införa fysiska säkerhetsåtgärder som minskar risken för insyn och obehörig observation under fjärrsessioner.

3.6 Uppfylla internationella regulatoriska krav för fjärråtkomst till data, inklusive GDPR, NIS2 och DORA.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner denna policy och säkerställer att den är tillräckligt resursförsedd samt integrerad i HR-, IT- och säkerhetsverksamheten.

4.1.2 Fastställer organisationens kriterier för behörighet till distansarbete och tillämplighet per verksamhetsenhet.

4.2 Informationssäkerhetschef (CISO) / ISMS-ansvarig

4.2.1 Ansvarar för policyn och dess förvaltning samt säkerställer att den är anpassad till organisationens riskbild och regulatoriska skyldigheter.

4.2.2 Fastställer säkerhetskontroller för fjärråtkomst, exempelvis kryptering, slutpunktsskydd och sessionstidsgränser.

4.2.3 Godkänner undantagshantering och övervakar kontrollernas effektivitet.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Granskningsfrekvens

9.1.1 Denna policy ska granskas årligen, eller oftare vid:

9.1.1.1 införande av ny teknik för fjärråtkomst

9.1.1.2 betydande utökning av distansarbete, exempelvis initiativ för hybridarbete

9.1.1.3 framväxt av nya hot, sårbarheter eller incidenter kopplade till distansmiljöer

9.1.1.4 förändringar i relevanta rättsliga eller regulatoriska ramverk

9.2 Ägarskap och granskningsprocess

9.2.1 Policyägare är informationssäkerhetschefen (CISO). Granskning ska samordnas med:

9.2.1.1 IT-drift och arkitektur

9.2.1.2 HR och fastighets- och tillgångsförvaltning avseende operativa konsekvenser och konsekvenser för arbetsplatsen

9.2.1.3 dataskyddsombudet avseende integritetsfrågor och gränsöverskridande datakontroller

9.2.2 Policyuppdateringar ska:

9.2.2.1 godkännas av styrgruppen för informationssäkerhet (ISSC)

9.2.2.2 kommuniceras till all berörd personal och berörda uppdragstagare

9.2.2.3 integreras i introduktionsmaterial och återkommande repetitionsutbildning

9.3 Dokumentstyrning och distribution

9.3.1 Policyn ska innehålla versionshantering, ikraftträdandedatum och ändringshistorik.

9.3.2 Ersatta versioner ska bevaras i enlighet med dokumenthanteringspolicyn (P14).

9.3.3 Reviderade versioner ska utlösa obligatorisk ny policybekräftelse för användare som är behöriga till distansarbete.

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer baslinjen för säker hantering av tillgångar och gäller för alla arbetsmiljöer, inklusive distansarbete.

10.1.2 P3 – Policy för godtagbar användning: Styr lämplig användning av organisationens enheter och system vid distansarbete.

10.1.3 P4 – Åtkomstkontrollpolicy: Säkerställer att åtkomstbehörigheter för fjärråtkomst följer principen om minsta privilegium och lämpliga autentiseringsmekanismer.

10.1.4 P6 – Riskhanteringspolicy: Fastställer hur risker kopplade till distansarbete identifieras, behandlas och övervakas inom ISMS.

10.1.5 P12 – Tillgångshanteringspolicy: Kräver tillgångsinventering och styrning av konfigurationsändringar för alla enheter som används på distans.

10.1.6 P22 – Loggnings- och övervakningspolicy: Säkerställer att fjärrsessioner övervakas, granskas och bevaras i enlighet med krav på regelefterlevnad.

10.1.7 P14 – Policy för datalagring och bortskaffande: Fastställer regler för datahantering som är relevanta för distansarbete, inklusive flyttbara medier och bortskaffande av enheter.

10.2 Dessa policyer säkerställer sammantaget att distansarbete är säkert, följer gällande krav och kan tillämpas inom samtliga funktioner och geografier.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända ramverk för säkerhet, dataskydd och IKT-riskhantering för att säkerställa säkra, spårbara och regelkonforma arbetssätt för distansarbete.

11.2 ISO/IEC 27001

11.2.1 Klausul 6.1.3 – planering av riskbehandling: Denna policy bidrar till behandling av risker kopplade till fjärråtkomst och distribuerade arbetsmiljöer.

11.2.2 Klausul 8.1 – operativ planering och styrning: Kräver införande av kontroller för system som används utanför organisationens lokaler.

11.2.3 Bilaga A, kontroll 6.7 – distansarbete: Denna policy täcker fullt ut nödvändiga informationssäkerhetskontroller när personal arbetar utanför organisationens lokaler, inklusive fysiska och logiska skydd, behörighetsstyrning och övervakning av användarbeteende.

11.3 ISO/IEC 27002:2022 – Kontroll 6

11.3.1 Denna kontroll kräver administrativa och tekniska skyddsåtgärder för distansarbete. Den omfattar krav på enhetssäkerhet, åtkomstmetoder, datahantering, miljörelaterade skyddsåtgärder och hantering av involverade tredje parter, vilket genomförs genom denna policy.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): Stöds direkt genom VPN-kontroller, MFA, sessionsloggning och rollbaserat godkännande av fjärråtkomst för användare som arbetar på distans.

11.4.2 AC-2 (Account Management): Styr behörighet för åtkomst, tilldelning av rättigheter för fjärråtkomst och avaktivering av konton.

11.4.3 SC-12 till SC-13 (Cryptographic Protection, Cryptographic Key Establishment): Genomförs genom obligatorisk användning av VPN och heldiskkryptering för slutpunkter som används på distans.

11.4.4 MP-5 (Media Transport Protection) och PE-18 (Location of Information System Components): Vägledning för distansarbete kräver skydd vid transport och fysiska skyddsåtgärder i miljöer utanför organisationens lokaler.

11.4.5 AU-2, AU-6: Loggning och övervakning av fjärrsessioner stödjer krav på revision och incidenthantering.

11.5 GDPR (EU) 2016/679

11.5.1 Artikel 32 – säkerhet i behandlingen: Denna policy säkerställer säkerhetskontroller för fjärråtkomst, kryptering och loggning som krävs för att skydda personuppgifter som nås eller behandlas på distans.

11.5.2 Artikel 5.1 f: Säkerställer att personuppgifter som nås utanför organisationens lokaler skyddas mot obehörig eller otillåten behandling samt oavsiktlig förlust.

11.5.3 Skäl 39: Betonar begränsning av åtkomst, riktighet och konfidentialitet, särskilt när enheter lämnar säkra lokaler.

11.6 NIS2-direktivet (EU) 2022/2555

11.6.1 Artikel 21.2 a, b, d: Kräver att fjärråtkomst skyddas som en del av organisationens ramverk för IKT-riskhantering. Denna policy uppfyller kravet på säkerhetsåtgärder som omfattar åtkomstkontroll, datasäkerhet och organisatoriska policyer för distansmiljöer.

11.6.2 Artikel 21.3: Främjar säkerhetsmedvetenhet och tillämpning av policyer bland personal som arbetar utanför centrala lokaler.

11.7 DORA-förordningen (EU) 2022/2554

11.7.1 Artikel 5 – styrning och ramverk för intern kontroll: Denna policy stödjer kraven på kontroll av IKT-risker i alla operativa scenarier, inklusive hybrida och distribuerade arbetsmodeller.

11.7.2 Artikel 8 – ramverk för IKT-riskhantering: Risker relaterade till fjärråtkomst identifieras, reduceras och styrs genom de tekniska och organisatoriska kontroller som anges här.

11.7.3 Artikel 9 – arrangemang för informationsdelning: Skyddar mot att information som delas inom nätverk för digital operativ motståndskraft läcker vid distansarbete.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Denna policy stödjer säker kontinuitet i verksamheten oavsett fysisk plats.

11.8.2 BAI06 – Managed IT Changes och BAI09 – Managed Assets: Säkerställer att enheter för distansarbete spåras, konfigureras säkert och hanteras som kritiska tillgångar.

11.8.3 APO13 – Managed Security: Främjar ett definierat ramverk för säkerhetsstyrning i distansmiljöer.

11.8.4 MEA03 – övervaka, utvärdera och bedöma efterlevnad: Fastställer att aktiviteter inom distansarbete ska loggas, granskas och revideras.