					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P09S					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**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroll 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU:s NIS2-direktiv	Artikel 21(2)(b), 21(2)(h)	EU:s NIS2-direktiv
EU:s DORA-förordning	Artikel 9	EU:s DORA-förordning
COBIT 2019	DSS05, APO13	COBIT 2019
EU:s GDPR	Artikel 32	EU:s GDPR

1. Syfte

1.1 Denna policy fastställer säkerhetskrav för anställda, entreprenörer och tredjepartsleverantörer som arbetar på distans, inklusive från hemmet, delade arbetsytor eller under resa.

1.2 Syftet är att skydda konfidentialitet, riktighet och tillgänglighet för verksamhetsinformation som nås utanför miljöer som kontrolleras av organisationen.

1.3 Denna policy säkerställer efterlevnad av internationella standarder och minskar risker såsom obehörig åtkomst, dataförlust och tjänsteavbrott.

2. Omfattning

2.1 Denna policy gäller för alla medarbetare (anställda, entreprenörer, tredjepartsleverantörer, konsulter och tillfälligt anställda) som får åtkomst till organisationens system, nätverk eller data vid arbete utanför arbetsplatsen.

2.2 Den omfattar:

2.2.1 Användning av enheter som tillhandahålls av organisationen och personligt ägda enheter

2.2.2 Åtkomst via VPN, fjärrskrivbord eller molntjänster

2.2.3 Säker hantering av information utanför organisationens lokaler

2.2.4 Övervakning, undantagshantering och tillämpning

2.3 Den gäller både heltids- och deltidsarrangemang för distansarbete, inklusive tillfällig fjärråtkomst.

3. Mål

3.1 Förhindra obehörig åtkomst till organisationens system eller känsliga data vid distansarbete.

3.2 Säkerställa att enheter och kommunikationsförbindelser som används utanför kontoret uppfyller kraven på säkerhetsbaslinje.

3.3 Upprätthålla kontroll över åtkomsträttigheter för fjärråtkomst och övervakning.

3.4 Ge tydlig vägledning till anställda och chefer om säkra arbetssätt för distansarbete.

3.5 Uppfylla förväntningar enligt ISO, NIS2, GDPR, DORA och COBIT för distansarbete och mobilt arbete.

4. Roller och ansvar

4.1 Verkställande direktör

4.1.1 Godkänner arrangemang för distansarbete och följer upp efterlevnaden.

4.1.2 Eskalerar säkerhetsincidenter eller upprepad bristande efterlevnad.

4.1.3 Granskar undantag och säkerställer uppföljning av incidenter.

4.2 IT-support eller externa IT-tjänsteleverantörer

4.2.1 Etablerar säker fjärråtkomst (t.ex. VPN och multifaktorautentisering (MFA)).

4.2.2 Upprätthåller endpointskydd, kryptering och säkerhetskonfiguration för enheter.

4.2.3 Stödjer användare och utreder tekniska säkerhetsproblem.

[... 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 Årlig policygranskning

9.1.1 Verkställande direktör och IT-support ska granska denna policy årligen för att anpassa den till förändringar i teknik, arbetsformer och rättsliga krav.

9.2 Utlösande faktorer för tidigare uppdatering

9.2.1 Omedelbar granskning krävs efter:

9.2.1.1 Större säkerhetsincident vid distansarbete

9.2.1.2 Ändringar i krav enligt NIS2, GDPR eller DORA

9.2.1.3 Övergång till ny teknik för fjärråtkomst (t.ex. annan VPN-plattform)

9.3 Versionshantering och arkivering

9.3.1 Alla versioner av denna policy ska:

9.3.1.1 Vara daterade och godkända av verkställande direktör

9.3.1.2 Vara försedda med versionsnummer

9.3.1.3 Arkiveras i minst tre år

9.4 Kommunikation till personal

9.4.1 Uppdateringar av policyn ska kommuniceras till alla distansanvändare. Bekräftelse krävs vid varje väsentlig ändring.

10. Relaterade policyer och kopplingar

10.1 Denna policy är kopplad till och stödjer följande:

10.1.1 P2S – Policy för styrningsroller och ansvar: Definierar vem som godkänner och utövar tillsyn över fjärråtkomst

10.1.2 P4S – Policy för åtkomstkontroll: Fastställer säker konfiguration av fjärråtkomst och rutiner för borttagning av behörigheter

10.1.3 P6S – Policy för riskhantering: Följer upp och utvärderar risker relaterade till åtkomst utanför arbetsplatsen

10.1.4 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Utbildar användare om risker vid distansarbete och god praxis

10.1.5 P30S – Policy för incidenthantering: Hanterar åtgärder vid incidenter kopplade till fjärråtkomst, såsom läckage av autentiseringsuppgifter eller förlust av enhet

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Riskbaserad planering för scenarier med fjärråtkomst

11.1.2 Klausul 6.2 – Behandlar ansvar inom HR i mobila och distribuerade arbetsformer

11.1.3 Klausul 8.1 – Operativ planering och styrning av processer för distansarbete

11.2 ISO/IEC 27002

11.2.1 Kontroll 6.7 – Ger praktisk vägledning om säkerhet för distansarbete och mobilt arbete

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Styrning av fjärråtkomst, sessionsskydd och säkerhetsövervakning

11.3.2 AC-2 – Kontostyrning för användare utanför arbetsplatsen

11.4 EU:s GDPR

11.4.1 Artikel 32 – Kräver dataskydd ”genom design och som standard”, inklusive i distansmiljöer

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(b) – Kräver säker användning av nätverks- och informationssystem

11.5.2 Artikel 21(2)(h) – Ställer krav på HR-relaterade säkerhetsåtgärder, inklusive kontroller utanför arbetsplatsen

11.6 EU:s DORA-förordning

11.6.1 Artikel 9 – Kräver att finansiella entiteter upprätthåller motståndskraft i IKT-system i alla operativa lägen, inklusive fjärråtkomst

11.7 COBIT 2019

11.7.1 DSS05 – Hantera säkerhetstjänster: Omfattar endpointskydd och säkra arbetssätt för distansarbete

11.7.2 APO13 – Hanterad säkerhet: Säkerställer säker tilldelning av åtkomst och tillsyn över risker för mobil åtkomst och fjärråtkomst