					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P10					Dokumenttitel: **Policy för rent skrivbord och låst skärm**							
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 6.1.3, klausul 8	riskbehandlingsplan, operativ planering och styrning för säkra arbetsytor
ISO/IEC 27002:2022	Kontroll 7	beteendemässiga och miljörelaterade kontroller för att skydda obevakad fysisk information
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fysiskt tillträde, säkerhet för entreprenörer, mediesanering, sessionslåsning samt konfigurations- och autentiseringskontroller
EU:s GDPR	Artiklarna 5.1 f och 32; skäl 39	dataintegritet, konfidentialitet och fysiska skyddsåtgärder för data
EU:s NIS2-direktiv	Artiklarna 21.2 d och 21.3	policyer för fysisk säkerhet, användarbeteende och förebyggande av dataläckage
EU:s DORA-förordning	Artiklarna 5, 8, 9	intern styrning, IKT och incidenthantering som omfattar fysisk säkerhet
COBIT 2019	DSS01, DSS05, MEA	hanterad drift, säkerhetstjänster och övervakning av efterlevnad

1. Syfte

1.1 Denna policy fastställer obligatoriska kontroller för att skydda känslig information genom att kräva säker hantering av fysiska dokument, arbetsstationer, skärmar och flyttbara medier i såväl kontorsmiljöer som delade arbetsytor.

1.2 Den stödjer ISO/IEC 27001 bilaga A, kontroll 7.7, genom att tillämpa beteendemässiga och tekniska arbetssätt som minskar risken för obehörigt röjande, stöld eller förlust av data till följd av obevakad eller synlig information.

1.3 Policyn stärker fysisk säkerhet och informationssäkerhet i den dagliga verksamheten och stödjer efterlevnad av tillämpliga rättsliga skyldigheter, avtalskrav och regulatoriska krav.

2. Omfattning

2.1 Denna policy gäller all personal som arbetar i eller har åtkomst till fysiska arbetsytor, inklusive:

2.1.1 Tillsvidareanställda och tillfälligt anställda

2.1.2 Entreprenörer, konsulter, leverantörer och praktikanter

2.1.3 Tredjepartsleverantörer och besökare på plats med åtkomst till känslig information

2.2 Kraven gäller i:

2.2.1 Enskilda kontor, arbetsbås och öppna kontorslandskap

2.2.2 Mötesrum och delade samarbetsytor

2.2.3 Skrivarstationer, receptionsdiskar och kopieringsrum

2.2.4 Områden där fjärrarbetsstationer eller delade terminaler används

2.3 Policyn gäller även för tillfälliga eller hybrida arbetsmiljöer, till exempel aktivitetsbaserade arbetsplatser, samt miljöer med publik exponering där det finns risk för insyn eller obevakade data.

3. Mål

3.1 Att förhindra obehörig åtkomst till konfidentiell, känslig eller reglerad information som lämnas exponerad i fysisk eller digital form.

3.2 Att främja en standardiserad säkerhetsnivå i alla arbetsmiljöer genom användning av fysiska skyddsåtgärder, arbetsstationskonfiguration och slutanvändarbeteende.

3.3 Att minska risken för integritetsincidenter, förlust av immateriella rättigheter och dataexfiltration som orsakas av oaktsamhet eller bristande tillsyn.

3.4 Att förankra arbetssätt för rent skrivbord och låst skärm i organisationens informationssäkerhetskultur för att stödja operativ disciplin, revisionsbarhet och regulatorisk försvarbarhet.

3.5 Att stödja efterlevnad av ISO/IEC 27001, artikel 32 i GDPR, artikel 15 i NIS2 och andra krav på fysisk säkerhet som är relevanta för kritiska data eller personuppgifter.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner denna policy och främjar en säkerhetsmedveten kultur i samtliga verksamhetsenheter.

4.1.2 Avsätter lämpliga resurser för tillämpning av policyn, medvetandehöjande insatser och fysiska kontrollmekanismer.

4.2 Informationssäkerhetschef (CISO) / ISMS-ansvarig

4.2.1 Är policyägare för denna policy och säkerställer att den är anpassad till ISO/IEC 27001:2022, revisionskrav och riskbehandlingsstrategier.

4.2.2 Tar fram utbildnings- och medvetandehöjande program samt kontroller för att säkerställa ett enhetligt genomförande i lokaler och hybrida arbetsmiljöer.

4.2.3 Samordnar med fastighetsfunktionen och IT för att säkerställa att lämpliga fysiska skyddsåtgärder finns på plats.

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

9. Krav på granskning och uppdatering

9.1 Schema för policygranskning

9.1.1 Denna policy ska granskas:

9.1.1.1 Minst årligen

9.1.1.2 Efter varje revisionsavvikelse som rör exponering i arbetsytor eller på skärmar

9.1.1.3 Efter en fysisk eller miljörelaterad incident, till exempel stöld av enhet, obehörig medpassage eller övervakning

9.1.1.4 Vid införande av nya kontorslayouter, lokala riktlinjer eller arbetsplatsmodeller, till exempel aktivitetsbaserat arbete eller distanshubbar

9.2 Ansvariga ägare

9.2.1 Policyägare är informationssäkerhetschef (CISO) eller utsedd ISMS-ansvarig.

9.2.2 Granskningsprocessen ska omfatta:

9.2.2.1 Fastighetsfunktion och fysisk säkerhet

9.2.2.2 IT och infrastruktur för teknisk tillämpning kopplad till enheter

9.2.2.3 HR och juridisk funktion för beteendestyrning och anpassning av disciplinära åtgärder

9.2.3 Alla policyuppdateringar ska versionshanteras, godkännas av styrgruppen för informationssäkerhet (ISSC) och återdistribueras med förnyad policybekräftelse där så krävs.

9.3 Kommunikation av ändringar

9.3.1 Användare ska informeras om väsentliga uppdateringar via:

9.3.1.1 Intranätets policycenter eller portal

9.3.1.2 Riktad e-postkommunikation

9.3.1.3 Repetitionsmoment vid introduktion och kvartalsvisa informationsgenomgångar

9.3.1.4 Obligatoriska bekräftelsemeddelanden för nya kritiska klausuler om tillämpning

10. Relaterade policyer och kopplingar

10.1 Denna policy är anpassad till och stödjer följande:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer förväntningar på användarbeteende och fysisk säkerhet som ligger till grund för denna policy.

10.1.2 P3 – Policy för godtagbar användning: Behandlar användarnas ansvar för att skydda data och system, inklusive fysiska miljöer.

10.1.3 P6 – Riskhanteringspolicy: Inkluderar risker i fysiska arbetsytor som en del av organisationens övergripande analys av informationsrisker.

10.1.4 P12 – Policy för tillgångshantering: Stödjer spårning och säker hantering av enheter och medier som lämnas på skrivbord.

10.1.5 P13 – Policy för dataklassificering och märkning: Kopplar till tillämpning av rent skrivbord för fysiska dokument märkta Konfidentiell eller Intern.

10.1.6 P14 – Policy för bevarande och bortskaffande av data: Vägledande för bevarande av fysiska dokument, dokumentförstöring och hantering av behållare.

10.1.7 P22 – Loggnings- och övervakningspolicy: Kan användas för att övervaka status för arbetsstationslåsning, inaktivitetstid eller kameraflöden från arbetsytor där detta är tillåtet.

10.2 Dessa relaterade policyer etablerar en integrerad informationssäkerhetskultur som kombinerar användarmedvetenhet, fysiska skyddsåtgärder och ansvar för att säkerställa motståndskraftiga arbetsmiljöer.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till globalt erkända standarder och rättsliga krav som kräver skydd av känslig information i fysiska miljöer och genom användarbeteende.

11.2 ISO/IEC 27001

11.2.1 Klausul 6.1.3 – Riskbehandlingsplan: Stödjer genomförande av kontroller för att minska fysiska och miljörelaterade risker, inklusive sådana som är kopplade till användarbeteende i öppna arbetsmiljöer.

11.2.2 Klausul 8.1 – Operativ planering och styrning: Fastställer operativa skyddsåtgärder för att hantera säkra arbetsytor och användning av utrustning.

11.3 ISO/IEC 27002:2022 – Kontroll 7

11.3.1 Denna kontroll kräver beteendemässiga och miljörelaterade skyddsåtgärder för att förhindra obehörig åtkomst till information via obevakade medier, skärmar eller utskrivet material. Policyn tillämpar ordning och säkerhet i fysiska arbetsytor, användning av skärmlås och bortskaffande av känsliga dokument.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Behörigande av fysiskt tillträde): Knyts till begränsningar i arbetsytor och tillämpning av låst förvaring i högriskmiljöer.

11.4.2 PS-7 (Säkerhet för extern personal): Tillämpas genom krav på rent skrivbord och låst skärm som utsträcks till entreprenörer och tredjepartsanvändare.

11.4.3 MP-6 (Mediesanering) och AC-11 (Sessionslåsning): Genomförs genom rutiner för säkert bortskaffande och obligatoriska timerinställningar för skärmlåsning.

11.4.4 CM-6 (Konfigurationsinställningar) och IA-5 (Hantering av autentiserare): Stödjer teknisk tillämpning av skärmlåsning och sessionskontroll på slutpunkter.

11.5 EU:s GDPR (2016/679)

11.5.1 Artikel 5.1 f: Kräver riktighet och konfidentialitet för personuppgifter, inklusive skydd mot fysisk exponering eller visning för obehöriga personer.

11.5.2 Artikel 32 – Säkerhet i samband med behandling: Kräver lämpliga fysiska och organisatoriska åtgärder för att skydda personuppgifter mot oavsiktlig eller olaglig förstöring, förlust eller obehörigt röjande, vilket uppnås genom kontroller för skrivbord och skärm.

11.5.3 Skäl 39: Kräver att åtkomst till personuppgifter begränsas till behöriga personer, vilket även omfattar skydd i fysisk form när uppgifterna lämnas obevakade.

11.6 EU:s NIS2-direktiv (2022/2555)

11.6.1 Artikel 21.2 d: Kräver policyer och rutiner för fysisk säkerhet och miljösäkerhet, inklusive skydd av information på arbetsplatsnivå.

11.6.2 Artikel 21.3: Främjar en säkerhetskultur som omfattar gott användarbeteende, medvetenhet och förebyggande av oavsiktliga dataläckor, vilket stöds av denna policys beteendekontroller.

11.7 EU:s DORA-förordning (2022/2554)

11.7.1 Artikel 5 – Intern styrning och kontroll: Kräver att alla IKT-relaterade risker, inklusive mänskliga och miljörelaterade hot, styrs genom bindande policyer.

11.7.2 Artikel 8 – IKT-riskhantering: Kräver skyddsåtgärder i både digitala och fysiska sammanhang så att användare på distans, på filialer och lokalt inte skapar oövervakad exponering.

11.7.3 Artikel 9 – Incidenthantering: Kräver att miljörelaterade eller beteendemässiga brister som leder till exponering av data loggas, klassificeras och hanteras med lämpliga korrigerande åtgärder.

11.8 COBIT 2019

11.8.1 DSS01 – Hanterad drift: Säkerställer operativ disciplin för att skydda fysiska arbetsytor och system genom repeterbara kontroller.

11.8.2 DSS05 – Hanterade säkerhetstjänster: Stödjer skydd av data, enheter och åtkomstpunkter genom beteendebaserad tillämpning såsom arbetssätt för rent skrivbord.

11.8.3 MEA03 – Övervaka, utvärdera och bedöm efterlevnad: Främjar revision av fysiska skyddsåtgärder och tillämpning av policyn i den dagliga verksamheten.