					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P10S					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 tillämpliga standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 7.2, 8	
ISO/IEC 27002:2022	Kontroll 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
EU:s NIS2-direktiv	Artikel 21(2)(d)	
EU:s DORA-förordning	Artikel 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
GDPR	Artikel 32	

1. Syfte

1.1 Denna policy fastställer bindande krav för att upprätthålla en säker arbetsmiljö genom att säkerställa att skrivbord, arbetsstationer och bildskärmar hålls fria från synlig konfidentiell information när de lämnas utan tillsyn.

1.2 Syftet är att förhindra obehörig åtkomst till känslig information via obevakade utskrifter, olåsta skärmar eller felaktigt förvarade flyttbara lagringsmedier, både i fysiska kontorsmiljöer och på platser för distansarbete.

1.3 De rutiner för rent skrivbord och låst skärm som anges i denna policy stärker organisationens förmåga att uppfylla kraven för certifiering enligt ISO/IEC 27001 genom att minimera förebyggbara exponeringsrisker. Dessa rutiner bidrar även till att skapa förtroende hos kunder, partner och revisorer för att informationssäkerhet hanteras på ett systematiskt sätt, även i resursbegränsade miljöer.

1.4 Denna policy stödjer en kultur präglad av ansvarstagande och medvetenhet, så att all personal, oavsett roll eller teknisk kompetens, förstår sitt ansvar att skydda företagets och kundernas information mot visuell exponering, stöld eller förlust.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla anställda, uppdragstagare, tredjepartsleverantörer, praktikanter och tillfälligt anställda som använder företagsägda eller personligen tilldelade arbetsstationer, skrivbord eller mobila enheter

2.1.2 Alla fysiska platser som används för verksamheten, inklusive dedikerade kontor, coworking-miljöer samt arbetsplatser för distans- eller hemarbete

2.1.3 Alla digitala enheter med visningsfunktion, inklusive stationära datorer, bärbara datorer, surfplattor och externa bildskärmar som används för verksamhetsändamål

2.2 Policyn omfattar alla fysiska eller digitala tillgångar som kan visa, innehålla eller överföra känslig information, inklusive:

2.2.1 Utskrifter eller handskrivna anteckningar

2.2.2 USB-minnen, CD-skivor och externa hårddiskar

2.2.3 Mobiltelefoner som används för verksamhetskommunikation eller e-post

2.2.4 Datorskärmar och projektorer som är anslutna till arbetssystem

2.3 Denna policy gäller även utanför ordinarie arbetstid och under avvikande driftförhållanden (t.ex. underhåll efter ordinarie arbetstid eller arbete inom incidenthantering).

3. Mål

3.1 Att införa praktiska och konsekventa kontroller som säkerställer att ingen känslig information lämnas exponerad på skrivbord, skärmar eller i gemensamma utrymmen.

3.2 Att minimera risken för obehörig åtkomst, både från interna källor (t.ex. oavsiktlig åtkomst av andra anställda) och externa hot (t.ex. besökare, städpersonal eller uppdragstagare och tredjepartsleverantörer).

3.3 Att stödja begränsningar avseende fysisk och logisk åtkomst genom att kräva att personal aktivt skyddar arbetsmaterial och låser datorer när de lämnas utan tillsyn.

3.4 Att öka personalens medvetenhet om säkra arbetssätt och tillhandahålla enkla, bindande regler som kan tillämpas i den dagliga verksamheten, oavsett arbetsplats.

3.5 Att säkerställa anpassning till ISO/IEC 27001 bilaga A, kontroll 7.7, och tillhörande vägledning i ISO/IEC 27002 avseende krav på rent skrivbord och låst skärm.

3.6 Att säkerställa att organisationen kan visa tillbörlig aktsamhet och revisionsberedskap utan att kräva infrastruktur på enterprise-nivå.

4. Roller och ansvar

4.1 Verkställande chef (GM)

4.1.1 Äger denna policy och säkerställer att den kommuniceras korrekt, förstås och efterlevs av alla anställda, uppdragstagare och tredjepartsleverantörer.

4.1.2 Ansvarar för att godkänna undantag, hantera överträdelser och utöva tillsyn över utbildning kopplad till säkra arbetsrutiner.

4.1.3 Ska genomföra eller delegera regelbundna kontroller (minst kvartalsvis) för att bekräfta att fysiska och digitala arbetsytor uppfyller policyns krav.

4.2 Utsedd medarbetare (om sådan har utsetts)

4.2.1 Kan tilldelas ansvar för att genomföra tekniska konfigurationer (t.ex. inställningar för automatiskt skärmlås efter tidsgräns) eller tillhandahålla fysisk förvaringsutrustning (t.ex. låsbara lådor).

4.2.2 Stödjer GM genom att rapportera bristande efterlevnad, hantera påminnelser om säker arbetsyta och följa upp åtgärder när brister identifieras.

4.2.3 Bidrar till att säkerställa att alla anställda har tillgång till lämpliga låsmekanismer eller säkra förvaringsutrymmen där det är praktiskt möjligt.

[... 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 GM ska granska denna policy minst en gång per år och efter någon av följande händelser:

9.1.1 Införande av nya kontorsutrymmen, enheter eller delade system

9.1.2 Ändringar i tillämpliga rättsliga krav eller certifieringskrav

9.1.3 Iakttagelser från revisioner, riskbedömningar eller säkerhetsincidenter

9.2 Interimistiska uppdateringar ska kommuniceras till alla anställda via e-post, och bekräftelse krävs.

9.3 Tidigare versioner av denna policy ska förvaras säkert och vara tillgängliga för granskning för att visa fortlöpande anpassning till ISO/IEC 27001 och relaterade ramverk.

10. Relaterade policyer och kopplingar

10.1 P2S – Policy för styrningsroller och ansvar: Förtydligar GM:s befogenheter att tillämpa och följa upp beteenden i fysiska och digitala arbetsytor.

10.2 P4S – Policy för åtkomstkontroll: Stödjer det tekniska genomförandet av skärmlås och säker inloggning till arbetsstationer.

10.3 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Förstärker den beteendebaserade utbildning som krävs för policyefterlevnad.

10.4 P17S – Policy för dataskydd och integritet: Definierar skyldigheter för hantering och skydd av personuppgifter och känsliga data i enlighet med GDPR.

10.5 P30S – Policy för incidenthantering (P30): Tillhandahåller eskaleringsvägar och ramverk för incidenthantering om en överträdelse leder till dataexponering eller personuppgiftsincident.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 7.2: Kräver att all personal är medveten om sina säkerhetsansvar, inklusive fysiska skyddsåtgärder.

11.1.2 Klausul 8.1: Operativa kontroller ska säkerställa ändamålsenligt fysiskt och logiskt skydd.

11.2 ISO/IEC 27002

11.2.1 Kontroll 7.7: Ger detaljerad vägledning om att fastställa, kommunicera och tillämpa krav på rent skrivbord och låst skärm.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Fastställer förväntningar på fysisk åtkomstsäkerhet, inklusive personalens beteende i säkra miljöer.

11.3.2 AC-11: Kräver sessionslåsning på arbetsstationer för att förhindra obehörig visning eller interaktion.

11.4 GDPR

11.4.1 Artikel 32: Kräver att organisationer skyddar personuppgifter genom fysiska och tekniska skyddsåtgärder, inklusive arbetsstationer och dokument.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(d): Kräver att organisationer inför riskbaserade policyer för fysisk och logisk åtkomst.

11.6 EU:s DORA-förordning

11.6.1 Artikel 9(2)(f): Kräver IKT-säkerhetskrav, inklusive säker hantering av arbetsytor, för aktörer inom den finansiella sektorn och deras leveranskedjor.

11.7 COBIT 2019

11.7.1 DSS01.06: Kräver rutiner för skydd av tillgångar, inklusive fysiska kontroller av arbetsytor och medier.

11.7.2 DSS05.02: Stödjer tillämpning av säkerhetsrutiner för slutanvändare i olika driftmiljöer.