					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P10S					Dokumenttitel: **Clean desk-politik og skærmpolitik**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

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

1. Formål

1.1 Denne politik fastsætter bindende retningslinjer for opretholdelse af et sikkert arbejdsmiljø ved at sikre, at skriveborde, arbejdsstationer og skærme holdes fri for synlige fortrolige oplysninger, når de er uden opsyn.

1.2 Hovedformålet er at forhindre uautoriseret adgang til følsomme oplysninger via print uden opsyn, ulåste skærme eller forkert opbevarede flytbare medier, både i fysiske kontormiljøer og ved fjernarbejde.

1.3 De clean desk- og skærmpraksisser, der er fastsat i denne politik, styrker organisationens evne til at opfylde kravene til ISO/IEC 27001-certificering ved at minimere forebyggelige risici for eksponering. Disse praksisser giver også kunder, partnere og revisorer sikkerhed for, at vi tager informationssikkerhed alvorligt, også i miljøer med begrænsede ressourcer.

1.4 Denne politik understøtter en kultur præget af ansvarlighed og bevidsthed og sikrer, at alt personale – uanset rolle eller teknisk ekspertise – forstår deres ansvar for at beskytte virksomheds- og kundeoplysninger mod visuel eksponering, tyveri eller tab.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, kontrahenter, praktikanter og midlertidigt ansatte, der anvender virksomhedsejede eller personligt tildelte arbejdsstationer, skriveborde eller mobile enheder

2.1.2 Alle fysiske lokationer, der anvendes til forretningsaktiviteter, herunder faste kontorer, coworking-miljøer og fjernarbejds-/hjemmearbejdspladser

2.1.3 Alle digitale enheder med visningsfunktioner, herunder stationære computere, bærbare computere, tablets og eksterne skærme, der anvendes til forretningsformål

2.2 Politikken omfatter alle fysiske eller digitale aktiver, der kan vise, indeholde eller overføre følsomme oplysninger, herunder:

2.2.1 Printede registreringer eller håndskrevne noter

2.2.2 USB-drev, cd'er og eksterne harddiske

2.2.3 Mobiltelefoner anvendt til forretningsrelaterede beskeder eller e-mail

2.2.4 Computerskærme og projektorer forbundet til arbejdssystemer

2.3 Denne politik gælder også uden for normal arbejdstid og under ikke-standardiserede driftsforhold, f.eks. ved vedligeholdelse uden for arbejdstid eller arbejde i forbindelse med hændelseshåndtering.

3. Mål

3.1 At håndhæve praktiske og ensartede sikkerhedskontroller, der sikrer, at ingen følsomme oplysninger efterlades synligt eksponeret på skriveborde, skærme eller i fællesområder.

3.2 At minimere risikoen for uautoriseret adgang, både fra interne kilder (f.eks. utilsigtet adgang fra andre medarbejdere) og eksterne trusler (f.eks. besøgende, rengøringspersonale eller kontrahenter).

3.3 At understøtte begrænsninger i fysisk og logisk adgang ved at kræve, at medarbejdere aktivt sikrer arbejdsmaterialer og låser computere, når de forlader dem uden opsyn.

3.4 At styrke medarbejdernes bevidsthed om sikker arbejdspraksis og fastsætte enkle, håndhævelige regler, der kan anvendes i den daglige drift uanset arbejdssted.

3.5 At sikre overensstemmelse med ISO/IEC 27001 Annex A kontrol 7.7 og den tilhørende implementeringsvejledning i ISO/IEC 27002 for krav til clean desk og skærm.

3.6 At sikre, at organisationen kan dokumentere rettidig omhu og revisionsberedskab uden krav om infrastruktur på enterprise-niveau.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Er ejer af denne politik og sikrer, at den kommunikeres korrekt, forstås og efterleves af alle medarbejdere og kontrahenter.

4.1.2 Er ansvarlig for at godkende eventuelle undtagelser, reagere på overtrædelser og føre tilsyn med træning relateret til sikker arbejdspraksis.

4.1.3 Skal gennemføre eller delegere regelmæssige kontroller (mindst kvartalsvist) for at bekræfte, at fysiske og digitale arbejdsmiljøer opfylder politikkens krav.

4.2 Udpeget medarbejder (hvis relevant)

4.2.1 Kan få ansvar for at implementere tekniske konfigurationer (f.eks. indstillinger for skærmtimeout) eller udlevere fysiske opbevaringsløsninger (f.eks. aflåselige skuffer).

4.2.2 Understøtter GM ved at rapportere manglende efterlevelse, håndtere påmindelser om arbejdspladssikkerhed og følge op på afhjælpende handlinger, når der identificeres forhold.

4.2.3 Medvirker til at sikre, at alle medarbejdere har adgang til passende låsemekanismer eller sikre opbevaringsområder, hvor det er praktisk muligt.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 GM skal gennemgå denne politik mindst én gang årligt og efter en af følgende hændelser:

9.1.1 Indførelse af nye kontorområder, enheder eller delte systemer

9.1.2 Ændringer i gældende lovkrav eller certificeringskrav

9.1.3 Konstateringer fra revisioner, risikovurderinger eller sikkerhedshændelser

9.2 Midlertidige opdateringer skal kommunikeres til alle medarbejdere via e-mail, og bekræftelse er påkrævet.

9.3 Tidligere versioner af denne politik skal opbevares sikkert og være revisionssporbare for at dokumentere løbende overensstemmelse med ISO/IEC 27001 og relaterede rammeværk.

10. Relaterede politikker og sammenhænge

10.1 P2S – Politik for styringsroller og ansvarsområder: Præciserer GM's beføjelse til at håndhæve og revidere adfærd i fysiske og digitale arbejdsmiljøer.

10.2 P4S – Politik for adgangskontrol: Understøtter den tekniske implementering af skærmlås og sikker loginpraksis for arbejdsstationer.

10.3 P8S – Politik for informationssikkerhedsbevidsthed og -uddannelse: Understøtter den adfærdsmæssige træning, der er nødvendig for efterlevelse af politikken.

10.4 P17S – Politik for databeskyttelse og privatliv: Definerer forpligtelser ved håndtering og beskyttelse af personoplysninger og følsomme data i overensstemmelse med GDPR.

10.5 P30S – Politik for hændelsesrespons: Fastlægger rammerne for eskalering og respons, hvis en overtrædelse medfører dataeksponering eller brud.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 7.2: Kræver, at alle medarbejdere er bevidste om deres sikkerhedsansvar, herunder fysisk beskyttelse.

11.1.2 Klausul 8.1: Driftskontroller skal sikre passende fysisk og logisk beskyttelse.

11.2 ISO/IEC 27002

11.2.1 Kontrol 7.7: Giver detaljeret vejledning om etablering, kommunikation og håndhævelse af krav om clean desk og skærm.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Fastlægger forventninger til fysisk adgangsstyring, herunder personalets adfærd i sikre miljøer.

11.3.2 AC-11: Kræver sessionslåsefunktionalitet på arbejdsstationer for at forhindre uautoriseret visning eller interaktion.

11.4 EU GDPR

11.4.1 Artikel 32: Kræver, at organisationer beskytter personoplysninger ved hjælp af fysiske og tekniske sikkerhedsforanstaltninger, herunder arbejdsstationer og dokumenter.

11.5 EU NIS2-direktivet

11.5.1 Artikel 21(2)(d): Kræver, at organisationer implementerer risikobaserede politikker for fysisk og logisk adgang.

11.6 EU DORA

11.6.1 Artikel 9(2)(f): Kræver IKT-sikkerhedspolitikker, herunder sikker arbejdspladshygiejne, for aktører i den finansielle sektor og deres forsyningskæder.

11.7 COBIT 2019

11.7.1 DSS01.06: Kræver praksis for beskyttelse af aktiver, herunder fysiske kontroller for arbejdsområder og medier.

11.7.2 DSS05.02: Understøtter håndhævelse af sikkerhedspraksis for slutbrugere på tværs af driftsmiljøer.