					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P10					Dokumenttitel: **Politik for ryddeligt skrivebord og skærmlås**							
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	Afsnit 6.1.3, afsnit 8	risikobehandlingsplan, operationel planlægning og styring for sikre arbejdsområder
ISO/IEC 27002:2022	Kontrol 7	adfærdsmæssige og fysiske kontroller til sikring af ubeskyttede fysiske oplysninger
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fysisk adgang, sikkerhed for eksternt personale, bortskaffelse af medier, sessionslås, konfigurations- og autentifikatorstyring
EU GDPR	Artikel 5(1)(f), 32; betragtning 39	dataintegritet, fortrolighed og fysiske sikkerhedsforanstaltninger for data
EU NIS2	Artikel 21(2)(d), 21(3)	politikker for fysisk sikkerhed, brugeradfærd og forebyggelse af datalækage
EU DORA	Artikel 5, 8, 9	intern styring, IKT og hændelsesstyring, herunder fysisk sikkerhed
COBIT 2019	DSS01, DSS05, MEA	styrede driftsaktiviteter, sikkerhedstjenester og overvågning af efterlevelse

1. Formål

1.1 Denne politik fastsætter obligatoriske kontroller til beskyttelse af følsomme oplysninger ved at kræve sikker håndtering af fysiske dokumenter, arbejdsstationer, skærme og flytbare medier i både kontormiljøer og delte arbejdsområder.

1.2 Den understøtter ISO/IEC 27001 Annex A kontrol 7.7 ved at håndhæve adfærdsmæssige og tekniske praksisser, der reducerer risikoen for uautoriseret videregivelse, tyveri eller tab af data som følge af oplysninger, der er synlige eller efterladt uden opsyn.

1.3 Denne politik styrker fysisk sikkerhed og informationssikkerhed i den daglige drift og understøtter overholdelse af gældende juridiske, kontraktuelle og regulatoriske forpligtelser.

2. Omfang

2.1 Denne politik gælder for alle personer, der arbejder i eller har adgang til fysiske arbejdsområder, herunder:

2.1.1 Fastansatte og midlertidigt ansatte

2.1.2 Kontraktansatte, konsulenter, leverandører og praktikanter

2.1.3 Tredjepartsleverandører og besøgende på lokationen med adgang til følsomme oplysninger

2.2 Kravene gælder i:

2.2.1 Enkeltmandskontorer, kontorbåse og storrumskontorer

2.2.2 Mødelokaler og fælles samarbejdsområder

2.2.3 Printområder, receptionsområder og kopirum

2.2.4 Områder, hvor der anvendes fjernarbejdsstationer eller delte terminaler

2.3 Denne politik gælder også for midlertidige eller hybride arbejdsformer (f.eks. hot-desking) og offentligt tilgængelige miljøer, hvor der er risiko for skulderkig eller ubeskyttede data.

3. Mål

3.1 At forhindre uautoriseret adgang til fortrolige, følsomme eller regulerede oplysninger, der er efterladt eksponeret i fysisk eller digital form.

3.2 At fremme en standardiseret sikkerhedstilstand på tværs af alle arbejdsmiljøer gennem brug af fysiske sikkerhedsforanstaltninger, konfiguration af arbejdsstationer og slutbrugeradfærd.

3.3 At reducere risikoen for brud på databeskyttelsen, tab af immaterielle rettigheder og dataeksfiltrering som følge af uagtsomhed eller forglemmelse.

3.4 At forankre adfærd for ryddeligt skrivebord og ryddelig skærm i organisationens kultur med henblik på at understøtte driftsdisciplin, revisionssporbarhed og juridisk robusthed.

3.5 At understøtte overholdelse af ISO/IEC 27001, GDPR artikel 32, NIS2 artikel 15 og andre krav til fysisk sikkerhed, der er relevante for kritiske data eller personoplysninger.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og fremmer en sikkerhedsbevidst kultur på tværs af alle forretningsenheder.

4.1.2 Allokerer passende ressourcer til håndhævelse af politikken, awareness-kampagner og fysiske kontrolmekanismer.

4.2 CISO / ISMS-ansvarlig

4.2.1 Er ansvarlig for denne politik og sikrer dens tilpasning til ISO/IEC 27001:2022, revisionskrav og risikobehandlingsstrategier.

4.2.2 Udvikler awareness-programmer og kontroller for at sikre ensartet implementering på tværs af lokationer og hybride arbejdsformer.

4.2.3 Koordinerer med Facility Management og IT for at sikre, at relevante fysiske sikkerhedsforanstaltninger er etableret.

[... 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 Plan for gennemgang af politikken

9.1.1 Denne politik skal gennemgås:

9.1.1.1 Mindst én gang årligt

9.1.1.2 Efter enhver afvigelse konstateret ved revision, der vedrører eksponering af arbejdsområder eller skærme

9.1.1.3 Efter enhver fysisk eller miljømæssig hændelse (f.eks. tyveri af enhed, tailgating, overvågning)

9.1.1.4 Ved implementering af nye kontorlayout, facilitetsregler eller arbejdsområdemodeller (f.eks. hot-desking, fjernarbejdshubs)

9.2 Ansvarlige ejere

9.2.1 Politikejeren er CISO eller den udpegede ISMS-ansvarlige.

9.2.2 Gennemgangsprocessen skal involvere:

9.2.2.1 Teams for Facility Management og Corporate Security

9.2.2.2 IT og infrastruktur med henblik på håndhævelse relateret til enheder

9.2.2.3 HR og Jura med henblik på adfærdshåndhævelse og disciplinær tilpasning

9.2.3 Alle politikopdateringer skal versionsstyres, godkendes af Informationssikkerhedsstyregruppen (ISSC) og redistribueres med fornyet bekræftelse, hvor dette kræves.

9.3 Kommunikation af ændringer

9.3.1 Brugere skal underrettes om væsentlige opdateringer via:

9.3.1.1 Intranettets politikcenter eller portal

9.3.1.2 Målrettet e-mailkommunikation

9.3.1.3 Genopfriskning ved onboarding og kvartalsvise briefinger

9.3.1.4 Obligatoriske bekræftelsesprompter for nye kritiske håndhævelsesklausuler

10. Relaterede politikker og sammenhænge

10.1 Denne politik er tilpasset og understøtter følgende:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger forventninger til brugeradfærd og fysisk sikkerhed, som udgør grundlaget for denne politik.

10.1.2 P3 – Politik for acceptabel brug: Adresserer brugernes ansvar for beskyttelse af data og systemer, herunder fysiske miljøer.

10.1.3 P6 – Risikostyringspolitik: Indarbejder risici i fysiske arbejdsområder som en del af den samlede analyse af virksomhedens informationsrisici.

10.1.4 P12 – Politik for aktivstyring: Understøtter registrering og sikker håndtering af enheder og medier, der efterlades ved skriveborde.

10.1.5 P13 – Politik for dataklassificering og mærkning: Knytter håndhævelse af ryddeligt skrivebord til fysiske dokumenter mærket Fortrolig eller Intern.

10.1.6 P14 – Dataopbevaringspolitik: Vejleder om opbevaring, makulering og håndtering af beholdere til fysiske dokumenter.

10.1.7 P22 – Politik for logning og overvågning: Kan anvendes til at overvåge arbejdsstationers låsestatus, inaktiv tid eller kamerafeeds fra arbejdsområder, hvor dette er tilladt.

10.2 Disse relaterede politikker etablerer en integreret sikkerhedskultur, der kombinerer brugerbevidsthed, fysiske sikkerhedsforanstaltninger og ansvarlighed for at sikre robuste arbejdsområder.

11. Referencestandarder og rammeværk

11.1 Denne politik er tilpasset globalt anerkendte standarder og juridiske krav, som kræver beskyttelse af følsomme oplysninger i fysiske miljøer og gennem brugeradfærd.

11.2 ISO/IEC 27001

11.2.1 Afsnit 6.1.3 – risikobehandlingsplan: Understøtter implementering af kontroller til afbødning af fysiske og miljømæssige risici, herunder risici knyttet til brugeradfærd i åbne arbejdsområder.

11.2.2 Afsnit 8.1 – operationel planlægning og styring: Fastlægger operationelle sikkerhedsforanstaltninger til styring af sikre arbejdsområder og brug af udstyr.

11.3 ISO/IEC 27002:2022 – kontrol 7

11.3.1 Denne kontrol kræver adfærdsmæssige og miljømæssige beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til oplysninger via medier, skærme eller printede materialer uden opsyn. Politikken håndhæver fysisk orden i arbejdsområder, brug af skærmlås og bortskaffelse af følsomme dokumenter.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (godkendelser til fysisk adgang): Knyttet til begrænsninger i arbejdsområder og håndhævelse af aflåst opbevaring i højrisikomiljøer.

11.4.2 PS-7 (sikkerhed for eksternt personale): Anvendes gennem krav til ryddeligt skrivebord og skærm, som udvides til kontraktansatte og tredjepartsbrugere.

11.4.3 MP-6 (mediesanering) og AC-11 (sessionslås): Implementeret gennem procedurer for sikker bortskaffelse og obligatoriske timere for skærmlås.

11.4.4 CM-6 (konfigurationsindstillinger) og IA-5 (styring af autentifikatorer): Understøtter teknisk håndhævelse af skærmlås og sessionsstyring på endpoints.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 5(1)(f): Håndhæver integritet og fortrolighed for personoplysninger, herunder beskyttelse mod fysisk eksponering eller visning for uautoriserede personer.

11.5.2 Artikel 32 – behandlingssikkerhed: Kræver passende fysiske og organisatoriske foranstaltninger til beskyttelse af personoplysninger mod hændelig eller ulovlig tilintetgørelse, tab eller uautoriseret videregivelse — opnået gennem skrivebords- og skærmkontroller.

11.5.3 Betragtning 39: Kræver, at adgang til personoplysninger begrænses til autoriserede personer — dette omfatter sikring af oplysninger i fysisk form, når de er uden opsyn.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Artikel 21(2)(d): Kræver politikker og procedurer vedrørende fysisk sikkerhed og miljømæssig sikkerhed, herunder informationssikkerhedsbeskyttelse på arbejdspladsniveau.

11.6.2 Artikel 21(3): Fremmer en sikkerhedskultur, der omfatter god brugeradfærd, awareness og forebyggelse af utilsigtede datalækager — understøttet af denne politiks adfærdskontroller.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 – intern styring og kontrol: Kræver, at alle IKT-relaterede risici, herunder menneskelige og miljømæssige trusler, styres gennem håndhævelige politikker.

11.7.2 Artikel 8 – styring af IKT-risiko: Pålægger sikkerhedsforanstaltninger i både digitale og fysiske kontekster, så brugere med fjernadgang, filialbrugere og brugere i on-premises-infrastruktur ikke skaber uhåndteret eksponering.

11.7.3 Artikel 9 – hændelsesstyring: Kræver, at miljømæssige eller adfærdsmæssige svigt, som medfører dataeksponering, logges, klassificeres og håndteres med passende korrigerende handlinger.

11.8 COBIT 2019

11.8.1 DSS01 – styrede driftsaktiviteter: Sikrer driftsdisciplin i beskyttelsen af fysiske arbejdsområder og systemer gennem gentagelige kontroller.

11.8.2 DSS05 – styrede sikkerhedstjenester: Understøtter beskyttelse af data, enheder og adgangsendepunkter gennem adfærdsbaseret håndhævelse såsom praksis for ryddeligt skrivebord.

11.8.3 MEA03 – overvågning, evaluering og vurdering af overholdelse: Fremmer revision af fysiske sikkerhedsforanstaltninger og implementering af politikken i den daglige forretningspraksis.