					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P10					Documenttitel: **Beleid inzake opgeruimde werkplek en afgeschermd scherm**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 6.1.3, Clausule 8	risicobehandelingsplan, operationele planning en beheersing voor beveiligde werkplekken
ISO/IEC 27002:2022	Beheersmaatregel 7	gedragsmaatregelen en omgevingsbeheersmaatregelen ter beveiliging van onbeheerde fysieke informatie
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	fysieke toegang, beveiliging van externe medewerkers, afvoer van media, sessievergrendeling, configuratie-instellingen en beheer van authenticatiemiddelen
AVG	Artikelen 5(1)(f), 32; Overweging 39	gegevensintegriteit, vertrouwelijkheid en fysieke waarborgen voor gegevens
NIS2-richtlijn	Artikelen 21(2)(d), 21(3)	beleid voor fysieke beveiliging, gebruikersgedrag en preventie van datalekken
DORA	Artikelen 5, 8, 9	interne governance, ICT en incidentbeheer waarbij fysieke beveiliging betrokken is
COBIT 2019	DSS01, DSS05, MEA	beheerde operatie, beveiligingsdiensten en nalevingsmonitoring

1. Doel

1.1 Dit beleid stelt verplichte beheersmaatregelen vast ter bescherming van gevoelige informatie door veilige omgang te vereisen met fysieke documenten, werkstations, schermen en verwijderbare media in zowel kantooromgevingen als gedeelde werkruimten.

1.2 Dit beleid ondersteunt ISO/IEC 27001 Annex A, beheersmaatregel 7.7, door gedragsmaatregelen en technische praktijken af te dwingen die het risico op ongeautoriseerde openbaarmaking, diefstal of verlies van gegevens als gevolg van onbeheerde of zichtbare informatie beperken.

1.3 Dit beleid versterkt de fysieke beveiliging en informatiebeveiliging in de dagelijkse operatie en ondersteunt de naleving van toepasselijke wettelijke, contractuele en regelgevende verplichtingen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op al het personeel dat werkzaam is in of toegang heeft tot fysieke werkruimten, waaronder:

2.1.1 vaste en tijdelijke medewerkers

2.1.2 opdrachtnemers, consultants, leveranciers en stagiairs

2.1.3 externe dienstverleners en bezoekers op locatie met toegang tot gevoelige informatie

2.2 De vereisten zijn van toepassing op:

2.2.1 individuele kantoren, werkplekken en open kantoorruimten

2.2.2 vergaderruimten en gedeelde samenwerkingsruimten

2.2.3 printerlocaties, receptiebalies en kopieerruimten

2.2.4 locaties waar externe werkplekken of gedeelde kiosken worden gebruikt

2.3 Dit beleid is ook van toepassing op tijdelijke of hybride werkomgevingen (bijvoorbeeld hotdesking) en op publiek toegankelijke omgevingen waar risico bestaat op meekijken over de schouder of onbeheerde gegevens.

3. Doelstellingen

3.1 Het voorkomen van ongeautoriseerde toegang tot vertrouwelijke, gevoelige of gereguleerde informatie die in fysieke of digitale vorm zichtbaar of onbeveiligd is achtergelaten.

3.2 Het bevorderen van een gestandaardiseerde informatiebeveiligingshouding in alle werkomgevingen door middel van fysieke waarborgen, configuratie van werkstations en gedrag van eindgebruikers.

3.3 Het verminderen van het risico op privacyschendingen, verlies van intellectueel eigendom en data-exfiltratie als gevolg van nalatigheid of onoplettendheid.

3.4 Het verankeren van gedrag rond opgeruimde werkplekken en afgeschermde schermen in de organisatiecultuur ter ondersteuning van operationele discipline, auditeerbaarheid en juridische verdedigbaarheid.

3.5 Het ondersteunen van naleving van ISO/IEC 27001, AVG artikel 32, NIS2 artikel 15 en andere vereisten inzake fysieke beveiliging die relevant zijn voor kritieke gegevens of persoonsgegevens.

4. Rollen en verantwoordelijkheden

4.1 Topmanagement

4.1.1 Bekrachtigt dit beleid en bevordert een beveiligingsbewuste cultuur in alle bedrijfseenheden.

4.1.2 Stelt passende middelen beschikbaar voor handhaving van het beleid, bewustwordingscampagnes en fysieke beheersmaatregelen.

4.2 CISO / ISMS-manager

4.2.1 Is eigenaar van dit beleid en waarborgt afstemming op ISO/IEC 27001:2022, auditvereisten en risicobehandelingsstrategieën.

4.2.2 Ontwikkelt bewustwordingsprogramma's en beheersmaatregelen om een consistente implementatie binnen faciliteiten en hybride werkomgevingen te waarborgen.

4.2.3 Coördineert met Facilitair, assetmanagement en IT om te waarborgen dat passende fysieke waarborgen aanwezig zijn.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisatie

9.1 Planning van beleidsbeoordeling

9.1.1 Dit beleid moet worden beoordeeld:

9.1.1.1 ten minste jaarlijks

9.1.1.2 na iedere auditafwijking met betrekking tot blootstelling van werkruimten of schermen

9.1.1.3 na een fysiek of omgevingsincident (bijvoorbeeld diefstal van apparatuur, tailgating of observatie)

9.1.1.4 bij invoering van nieuwe kantoorindelingen, faciliteitsbeleid of werkplekmodellen (bijvoorbeeld hotdesking of remote hubs)

9.2 Verantwoordelijke eigenaren

9.2.1 De beleidseigenaar is de CISO of de aangewezen ISMS-manager.

9.2.2 Bij het beoordelingsproces moeten ten minste worden betrokken:

9.2.2.1 teams voor facilitair beheer en bedrijfsbeveiliging

9.2.2.2 IT en infrastructuur voor apparaatgerelateerde afdwinging

9.2.2.3 HR, Juridische Zaken en Compliance voor gedragsmatige handhaving en afstemming van disciplinaire maatregelen

9.2.3 Alle beleidsactualisaties moeten onder versiebeheer staan, worden goedgekeurd door de ISMS-stuurgroep en opnieuw worden verspreid met hernieuwde kennisname waar vereist.

9.3 Communicatie van wijzigingen

9.3.1 Gebruikers moeten op de hoogte worden gebracht van materiële wijzigingen via:

9.3.1.1 het intranetbeleidencentrum of portaal

9.3.1.2 gerichte e-mailcommunicatie

9.3.1.3 onboarding-opfrismomenten en kwartaalbriefings

9.3.1.4 verplichte kennisnameverzoeken voor nieuwe kritieke handhavingsclausules

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid is afgestemd op en ondersteunt het volgende:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt verwachtingen vast voor gebruikersgedrag en fysieke beveiliging die de basis vormen voor dit beleid.

10.1.2 P3 – Beleid inzake aanvaardbaar gebruik: behandelt de verantwoordelijkheid van gebruikers voor de bescherming van gegevens en systemen, inclusief fysieke omgevingen.

10.1.3 P6 – Risicobeheerbeleid: neemt risico's in fysieke werkruimten op als onderdeel van de organisatiebrede analyse van informatierisico's.

10.1.4 P12 – Assetmanagementbeleid: ondersteunt het volgen en de veilige omgang met apparaten en media die op bureaus worden achtergelaten.

10.1.5 P13 – Beleid inzake gegevensclassificatie en etikettering: legt de koppeling met handhaving van opgeruimde werkplekken voor fysieke documenten met het label Vertrouwelijk of Intern.

10.1.6 P14 – Gegevensbewarings- en afvoerbeleid: geeft richting aan de bewaring van fysieke documenten, versnippering en omgang met inzamelbakken.

10.1.7 P22 – Logging- en monitoringbeleid: kan worden gebruikt voor het monitoren van de vergrendelingsstatus van werkstations, inactieve tijd of camerabeelden van werkruimten waar dit is toegestaan.

10.2 Deze gerelateerde beleidslijnen leggen de basis voor een geïntegreerde beveiligingscultuur waarin gebruikersbewustzijn, fysieke waarborgen en verantwoordingsplicht samenkomen om weerbare werkruimten te waarborgen.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op wereldwijd erkende normen en wettelijke vereisten die bescherming van gevoelige informatie in fysieke omgevingen en via gebruikersgedrag verplicht stellen.

11.2 ISO/IEC 27001

11.2.1 Clausule 6.1.3 – Risicobehandelingsplan: ondersteunt de implementatie van beheersmaatregelen voor het beperken van fysieke en omgevingsrisico's, waaronder risico's die samenhangen met gebruikersgedrag in open werkruimten.

11.2.2 Clausule 8.1 – Operationele planning en beheersing: stelt operationele waarborgen vast om beveiligde werkruimten en het gebruik van apparatuur te beheersen.

11.3 ISO/IEC 27002:2022 – Beheersmaatregel 7

11.3.1 Deze beheersmaatregel vereist gedragsmaatregelen en omgevingsbeheersmaatregelen om ongeautoriseerde toegang tot informatie via onbeheerde media, schermen of geprinte materialen te voorkomen. Dit beleid dwingt werkplekhygiëne, schermvergrendeling en veilige afvoer van gevoelige documenten af.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (autorisaties voor fysieke toegang): gekoppeld via beperkingen op werkruimten en handhaving van afsluitbare opslag in omgevingen met een hoog risico.

11.4.2 PS-7 (beveiliging van extern personeel): toegepast via vereisten voor opgeruimde werkplekken en afgeschermde schermen die ook gelden voor opdrachtnemers en gebruikers van derde partijen.

11.4.3 MP-6 (sanering van media) en AC-11 (sessievergrendeling): geïmplementeerd via procedures voor veilige afvoer en verplichte timers voor schermvergrendeling.

11.4.4 CM-6 (configuratie-instellingen) en IA-5 (beheer van authenticatiemiddelen): ondersteunen technische afdwinging van schermvergrendeling en sessiebeheersing op endpoints.

11.5 AVG (2016/679)

11.5.1 Artikel 5(1)(f): dwingt integriteit en vertrouwelijkheid van persoonsgegevens af, inclusief bescherming tegen fysieke blootstelling of inzage door onbevoegde personen.

11.5.2 Artikel 32 – Beveiliging van de verwerking: vereist passende fysieke en organisatorische maatregelen om persoonsgegevens te beschermen tegen accidentele of onrechtmatige vernietiging, verlies of ongeautoriseerde openbaarmaking, gerealiseerd via beheersmaatregelen voor werkplekken en schermen.

11.5.3 Overweging 39: vereist dat toegang tot persoonsgegevens wordt beperkt tot bevoegde personen; dit omvat ook het beveiligen van persoonsgegevens in fysieke vorm wanneer deze onbeheerd zijn.

11.6 NIS2-richtlijn (2022/2555)

11.6.1 Artikel 21(2)(d): vereist beleidslijnen en procedures met betrekking tot fysieke beveiliging en omgevingsbeveiliging, waaronder bescherming van informatiebeveiliging op werkplekniveau.

11.6.2 Artikel 21(3): bevordert een beveiligingscultuur waarin goed gebruikersgedrag, bewustwording en preventie van onbedoelde datalekken zijn opgenomen, ondersteund door de gedragsmaatregelen van dit beleid.

11.7 DORA (2022/2554)

11.7.1 Artikel 5 – Interne governance en beheersing: vereist dat alle ICT-gerelateerde risico's, waaronder menselijke en omgevingsdreigingen, worden beheerst via afdwingbaar beleid.

11.7.2 Artikel 8 – ICT-risicomanagement: vereist waarborgen in zowel digitale als fysieke contexten, zodat gebruikers op afstand, op vestigingen en op locatie geen onbeheerde blootstelling veroorzaken.

11.7.3 Artikel 9 – Incidentbeheer: vereist dat omgevings- of gedragsfouten die leiden tot blootstelling van gegevens worden vastgelegd, geclassificeerd en aangepakt met passende corrigerende maatregelen.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: waarborgt operationele discipline bij de bescherming van fysieke werkruimten en systemen via herhaalbare beheersmaatregelen.

11.8.2 DSS05 – Managed Security Services: ondersteunt de bescherming van gegevens, apparaten en toegangsendpoints via gedragsgerichte handhaving zoals praktijken voor opgeruimde werkplekken.

11.8.3 MEA03 – Monitoren, evalueren en beoordelen van naleving: stimuleert auditing van fysieke waarborgen en toepassing van beleid in de dagelijkse bedrijfsvoering.