					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P10S					Documenttitel: **Beleid voor een opgeruimd bureau en een vergrendeld 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	Clausules 7.2, 8	
ISO/IEC 27002:2022	Beheersmaatregel 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	
AVG	Artikel 32	

1. Doel

1.1 Dit beleid stelt bindende richtlijnen vast voor het handhaven van een veilige werkomgeving door te waarborgen dat bureaus, werkplekken en beeldschermen geen zichtbaar vertrouwelijke informatie bevatten wanneer zij onbeheerd worden achtergelaten.

1.2 Het hoofddoel is het voorkomen van ongeautoriseerde toegang tot gevoelige informatie via onbeheerde afdrukken, niet-vergrendelde schermen of onjuist opgeborgen verwijderbare media, zowel in fysieke kantooromgevingen als op thuiswerk- en andere externe werklocaties.

1.3 De in dit beleid vastgelegde praktijken voor een opgeruimd bureau en een vergrendeld scherm versterken het vermogen van onze organisatie om te voldoen aan de certificeringseisen van ISO/IEC 27001 door vermijdbare blootstellingsrisico's tot een minimum te beperken. Deze praktijken geven klanten, partners en auditors bovendien vertrouwen dat wij informatiebeveiliging serieus nemen, ook in omgevingen met beperkte middelen.

1.4 Dit beleid ondersteunt een cultuur van verantwoordelijkheid en bewustzijn en waarborgt dat alle medewerkers, ongeacht hun rol of technische expertise, begrijpen dat zij verantwoordelijk zijn voor het beschermen van bedrijfs- en klantinformatie tegen visuele blootstelling, diefstal of verlies.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle werknemers, opdrachtnemers, stagiairs en tijdelijke krachten die gebruikmaken van werkstations, bureaus of mobiele apparaten die eigendom zijn van het bedrijf of persoonlijk aan hen zijn toegewezen

2.1.2 alle fysieke locaties die voor bedrijfsactiviteiten worden gebruikt, waaronder afzonderlijke kantoren, coworkingomgevingen en thuiswerk- of andere externe werkplekken

2.1.3 alle digitale apparaten met weergavemogelijkheden, waaronder desktops, laptops, tablets en externe monitoren die voor bedrijfsdoeleinden worden gebruikt

2.2 Het beleid is van toepassing op alle fysieke en digitale bedrijfsmiddelen die gevoelige informatie kunnen weergeven, bevatten of verzenden, waaronder:

2.2.1 geprinte documenten of handgeschreven notities

2.2.2 USB-sticks, cd's en externe harde schijven

2.2.3 mobiele telefoons die worden gebruikt voor zakelijke berichten of e-mail

2.2.4 computermonitoren en projectoren die zijn verbonden met werksystemen

2.3 Dit beleid blijft van toepassing buiten reguliere werktijden en tijdens niet-standaardwerkzaamheden, zoals onderhoud buiten kantooruren of werkzaamheden in het kader van een incidentrespons.

3. Doelstellingen

3.1 Het afdwingen van praktische en consistente beheersmaatregelen die waarborgen dat geen gevoelige informatie zichtbaar achterblijft op bureaus, schermen of in gemeenschappelijke ruimten.

3.2 Het minimaliseren van het risico op ongeautoriseerde toegang, zowel vanuit interne bronnen, zoals onbedoelde toegang door andere werknemers, als vanuit externe dreigingen, zoals bezoekers, schoonmaakpersoneel of opdrachtnemers.

3.3 Het ondersteunen van fysieke en logische toegangsbeperkingen door van medewerkers te eisen dat zij werkmaterialen actief beveiligen en computers vergrendelen wanneer deze onbeheerd worden achtergelaten.

3.4 Het vergroten van het bewustzijn van medewerkers over veilige werkpraktijken en het bieden van eenvoudige, afdwingbare regels die toepasbaar zijn in de dagelijkse bedrijfsvoering, ongeacht de werklocatie.

3.5 Het waarborgen van afstemming op ISO/IEC 27001 Bijlage A, beheersmaatregel 7.7, en de implementatierichtlijnen in ISO/IEC 27002 voor vereisten inzake een opgeruimd bureau en een vergrendeld scherm.

3.6 Het waarborgen dat de organisatie aantoonbare due diligence en auditgereedheid kan realiseren zonder infrastructuur op enterprise-niveau te vereisen.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Is eigenaar van dit beleid en ziet erop toe dat het correct wordt gecommuniceerd, begrepen en nageleefd door alle werknemers en opdrachtnemers.

4.1.2 Is verantwoordelijk voor het goedkeuren van uitzonderingen, het reageren op overtredingen en het toezicht op training met betrekking tot veilige werkpraktijken.

4.1.3 Voert regelmatig controles uit of delegeert deze, ten minste eenmaal per kwartaal, om te bevestigen dat fysieke en digitale werkplekken voldoen aan de verwachtingen van dit beleid.

4.2 Aangewezen medewerker (indien van toepassing)

4.2.1 Kan verantwoordelijk worden gesteld voor het implementeren van technische configuraties, zoals instellingen voor schermtime-out, of voor het beschikbaar stellen van fysieke beveiligingsmiddelen, zoals afsluitbare laden.

4.2.2 Ondersteunt de GM door niet-naleving te rapporteren, herinneringen over werkplekbeveiliging op te volgen en corrigerende maatregelen te monitoren wanneer problemen worden vastgesteld.

4.2.3 Helpt, waar haalbaar, te waarborgen dat alle werknemers toegang hebben tot passende vergrendelingsmechanismen of beveiligde opslagvoorzieningen.

[... 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 actualisering

9.1 De GM moet dit beleid ten minste eenmaal per jaar beoordelen en na elk van de volgende gebeurtenissen:

9.1.1 invoering van nieuwe kantoorruimten, apparaten of gedeelde systemen

9.1.2 wijzigingen in toepasselijke wettelijke vereisten of certificeringseisen

9.1.3 bevindingen uit audits, risicobeoordelingen of beveiligingsincidenten

9.2 Tussentijdse actualisaties moeten per e-mail aan alle werknemers worden gecommuniceerd, waarbij kennisname verplicht is.

9.3 Eerdere versies van dit beleid moeten veilig worden opgeslagen en auditeerbaar zijn om voortdurende afstemming op ISO/IEC 27001 en gerelateerde raamwerken aan te tonen.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: verduidelijkt de bevoegdheid van de GM om gedrag in fysieke en digitale werkplekken af te dwingen en te auditen.

10.2 P4S – Beleid inzake toegangsbeheersing: ondersteunt de technische implementatie van schermvergrendeling en veilige aanmeldpraktijken voor werkstations.

10.3 P8S – Beleid voor bewustwording en opleiding op het gebied van informatiebeveiliging: versterkt de gedragsgerichte training die nodig is voor naleving van dit beleid.

10.4 P17S – Beleid inzake gegevensbescherming en privacy: definieert verplichtingen voor de verwerking en bescherming van persoonsgegevens en gevoelige gegevens in overeenstemming met de AVG.

10.5 P30S – Incidentresponsbeleid: biedt het kader voor escalatie en respons wanneer een overtreding leidt tot blootstelling van gegevens of een datalek.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 7.2: vereist dat alle medewerkers zich bewust zijn van hun beveiligingsverantwoordelijkheden, waaronder fysieke beveiliging.

11.1.2 Clausule 8.1: operationele beheersmaatregelen moeten passende fysieke en logische beveiliging waarborgen.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 7.7: biedt gedetailleerde richtlijnen voor het vaststellen, communiceren en handhaven van vereisten voor een opgeruimd bureau en een vergrendeld scherm.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: stelt verwachtingen vast voor fysieke toegangsbeheersing, waaronder gedrag van personeel binnen beveiligde omgevingen.

11.3.2 AC-11: verplicht functionaliteit voor sessievergrendeling op werkstations om ongeautoriseerde inzage of interactie te voorkomen.

11.4 AVG

11.4.1 Artikel 32: vereist dat organisaties persoonsgegevens beschermen met fysieke en technische beveiligingsmaatregelen, waaronder werkstations en documenten.

11.5 NIS2-richtlijn

11.5.1 Artikel 21(2)(d): vereist dat organisaties risicogebaseerde beleidslijnen voor fysieke en logische toegang implementeren.

11.6 DORA

11.6.1 Artikel 9(2)(f): verplicht ICT-beveiligingsbeleid, waaronder veilige werkplekhygiëne, voor financiële instellingen en hun toeleveringsketens.

11.7 COBIT 2019

11.7.1 DSS01.06: vereist praktijken voor de bescherming van bedrijfsmiddelen, waaronder fysieke beheersmaatregelen voor werkplekken en media.

11.7.2 DSS05.02: ondersteunt de handhaving van eindgebruikerspraktijken inzake beveiliging in verschillende operationele omgevingen.