					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P33S					Documenttitel: **Beleid inzake audit- en nalevingsmonitoring**							
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 9.2, 10	Interne audits, continue verbetering en herstel van non-conformiteiten
ISO/IEC 27002:2022	Beheersmaatregelen 5.35, 5.37	Geplande interne beoordelingen, onafhankelijke beoordelingen van uitbestede processen
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Beveiligingsbeoordelingen, continue nalevingsmonitoring, auditbeoordeling, -analyse en -rapportage
AVG	Artikelen 24 en 32	Auditing van technische en organisatorische maatregelen, aantoonbaarheid van de doeltreffendheid van beheersmaatregelen
NIS2	Artikel 21(2)(f)	Proactieve beoordeling en op bewijs gebaseerde naleving
DORA	Artikel 10	ICT-risicobeheer, monitoring en rapportage
COBIT 2019	MEA01, MEA03	Monitoren, evalueren en beoordelen van conformiteit en naleving, gereedheid voor beoordelingen door derden

1. Doel

1.1 Dit beleid stelt de aanpak van de organisatie vast voor de uitvoering van interne audits, toetsing van beveiligingsmaatregelen en monitoring van naleving van wet- en regelgeving. Het waarborgt dat alle beheersmaatregelen, beleidslijnen, systemen en dienstverleners periodiek en gestructureerd worden beoordeeld.

1.2 Het doel is om het falen van beheersmaatregelen tijdig te detecteren, niet-naleving te voorkomen en due diligence aan te tonen onder ISO/IEC 27001, de AVG en aanverwante raamwerken.

1.3 Dit beleid stelt mkb-organisaties in staat de operationele beheersing en certificeringsgereedheid te behouden, ook zonder afzonderlijke compliancefunctie, door gebruik te maken van eenvoudige, herhaalbare checklists en op risico gebaseerde prioritering van bevindingen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle interne afdelingen en externe dienstverleners met verantwoordelijkheden met betrekking tot IT-systemen, persoonsgegevens en bedrijfskritische diensten

2.1.2 Alle beheersmaatregelen en systemen binnen de reikwijdte van het managementsysteem voor informatiebeveiliging (ISMS)

2.1.3 Alle interne audits, beoordelingen van beveiligingsmaatregelen en nalevingscontroles, ongeacht of deze intern of door een externe complianceadviseur, klant of toezichthouder worden uitgevoerd

2.2 Dit beleid is ook van toepassing op bewijsverzameling en rapportage ten behoeve van:

2.2.1 ISO/IEC 27001-certificerings- en hercertificeringsaudits

2.2.2 Gegevensbeschermingsaudits op grond van de AVG of contractuele verplichtingen

2.2.3 Door klanten geïnitieerde beveiligingsvragenlijsten of due diligence-beoordelingen

2.2.4 Eventuele toezichthoudende of onafhankelijke beoordelingen onder NIS2 of DORA, waar van toepassing

3. Doelstellingen

3.1 Waarborgen dat alle belangrijkste beheersmaatregelen en beleidslijnen periodiek worden beoordeeld op doeltreffendheid en naleving.

3.2 Audittrails en registraties van corrigerende maatregelen bijhouden om verantwoording en continue verbetering aan te tonen.

3.3 Voorbereiden op certificering, hercertificering en assuranceprogramma's richting klanten, bijvoorbeeld ISO 27001 en leveranciersonboarding.

3.4 Hiaten vroegtijdig identificeren, zodat tijdige remediatie mogelijk is voordat kwesties escaleren of verplichtingen worden geschonden.

3.5 De algemeen directeur en de IT-beheerder in staat stellen beoordelingen met minimale complexiteit te coördineren, met behoud van aantoonbaar verdedigbare uitkomsten.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Houdt toezicht op het auditprogramma

4.1.2 Keurt interne beoordelingsplannen en bevindingen goed

4.1.3 Wijst corrigerende maatregelen toe en bewaakt de opvolging

4.1.4 Geeft toestemming voor het inschakelen van externe auditors of adviseurs

4.2 IT-beheerder / IT-supportverlener

4.2.1 Levert bewijsmateriaal aan tijdens interne en externe audits, zoals logboeken, configuraties en registraties van toegangsbeheer

4.2.2 Ondersteunt bij technische controles, zoals back-upstatus en naleving van patchvereisten

4.2.3 Beheert de centrale opslaglocatie voor auditbewijsmateriaal

[... 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 Jaarlijkse beoordeling van beleid en auditplan

9.1.1 De algemeen directeur (GM) moet dit beleid en het auditschema ten minste eenmaal per jaar beoordelen.

9.1.2 Bij de beoordeling moet het volgende worden geëvalueerd:

9.1.2.1 De doeltreffendheid van audits bij het identificeren van hiaten

9.1.2.2 Het voltooiingspercentage van audits en corrigerende maatregelen

9.1.2.3 Wijzigingen in toepasselijke wettelijke, toezichthoudende of certificeringsvereisten

9.2 Gebeurtenisgestuurde actualisaties

9.2.1 Het beleid moet worden beoordeeld en bijgewerkt wanneer:

9.2.2 Een certificeringsaudit of controleaudit leidt tot een majeure non-conformiteit

9.2.3 Wettelijke of toezichthoudende kaders wijzigen, bijvoorbeeld nieuwe AVG-richtsnoeren of nationale implementatie van NIS2

9.2.4 Bedrijfswijzigingen invloed hebben op systemen, processen of leveranciers die binnen de auditreikwijdte vallen

9.2.5 Een kritiek incident of een inbreuk eerder niet-onderkende hiaten in beheersmaatregelen aan het licht brengt

9.3 Documentatie van actualisaties

9.3.1 Alle revisies moeten worden bijgehouden in een versiebeheerlogboek voor beleid.

9.3.2 Actualisaties moeten worden verspreid onder alle teamleden die bij audits betrokken zijn.

9.3.3 Bij het bijgewerkte beleid moet een samenvatting van wijzigingen worden gevoegd om begrip te waarborgen.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid wordt ondersteund door en versterkt verschillende andere mkb-beleidslijnen:

10.1.1 P1S – Informatiebeveiligingsbeleid: Stelt de basis vast voor alle verwachtingen ten aanzien van beheersmaatregelen en vereist handhaving via audits.

10.1.2 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: Legt verantwoording vast voor auditplanning, uitvoering en eigenaarschap van corrigerende maatregelen.

10.1.3 P6S – Beleid inzake risicobeheer: Identificeert zwakke plekken in beheersmaatregelen die tijdens audits aan het licht komen en waarborgt dat bevindingen in het risicoregister worden vastgelegd.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: Definieert de AVG-beheersmaatregelen die moeten worden geaudit, waaronder gegevensverwerking, respons op datalekken en privacyverklaringen.

10.1.5 P22S – Logging- en monitoringbeleid: Levert de auditlogs en forensische gegevens die worden gebruikt tijdens nalevings- en beheersingsbeoordelingen.

10.1.6 P30S – Incidentresponsbeleid (P30): Vereist periodieke audit van incidentregistraties en evaluaties na incidenten om de doeltreffendheid van de respons te verifiëren.

10.1.7 P31S – Beleid inzake bewijsverzameling en forensisch onderzoek: Biedt procedures voor het verzamelen van verifieerbaar bewijsmateriaal met chain of custody tijdens audits.

10.2 Samen vormen deze beleidslijnen een gesloten beheersingsomgeving die interne verificatie, externe assurance en op normen afgestemde informatiebeveiligingsgovernance mogelijk maakt.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:

11.1.1 Clausule 9.2 – Vereist interne audits om de prestaties van het ISMS en de afstemming op vereisten te evalueren.

11.1.2 Clausule 10.1 – Verplicht continue verbetering op basis van auditresultaten en herstel van non-conformiteiten.

11.2 ISO/IEC 27002:

11.2.1 Beheersmaatregel 5.35 – Vereist geplande interne beoordelingen van beheersmaatregelen en processen.

11.2.2 Beheersmaatregel 5.37 – Benadrukt onafhankelijke beoordelingen, in het bijzonder van uitbestede processen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Beveiligingsbeoordelingen: Vereist audits van geïmplementeerde beheersmaatregelen om de doeltreffendheid te verifiëren.

11.3.2 CA-7 – Continue nalevingsmonitoring: Benadrukt proactieve detectie en beoordeling van tekortkomingen in beheersmaatregelen.

11.3.3 AU-6 – Auditbeoordeling, analyse en rapportage: Verplicht regelmatige analyse en afhandeling van auditlogs en bevindingen.

11.4 AVG:

11.4.1 Artikelen 24 en 32 – Vereisen implementatie en auditing van technische en organisatorische maatregelen, met inbegrip van bewijsmateriaal voor de doeltreffendheid van beheersmaatregelen en verbetering in de tijd.

11.5 NIS2-richtlijn (2022/2555):

11.5.1 Artikelen 20–21 – Verplichten proactieve beoordeling van beheersmaatregelen, op bewijs gebaseerde naleving en auditeerbaarheid voor essentiële en belangrijke entiteiten.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitoren, evalueren en beoordelen van prestaties en conformiteit: Vereist periodieke beoordeling van procesprestaties en beheersmaatregelen ten opzichte van normen en doelstellingen.

11.6.2 MEA03 – Naleving van externe vereisten waarborgen: Richt zich op interne monitoring en gereedheid voor audits door derden en beoordelingen door toezichthouders.