					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P29S					Documenttitel: **Beleid inzake testgegevens en testomgevingen**							
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 6.1, 8	
ISO/IEC 27002:2022	Beheersmaatregelen 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
AVG	Artikelen 5(1)(c), 25, 32	
EU NIS2	Artikel 21(2)(e), (h)	
EU DORA	Artikel 9	
COBIT 2019	BAI07, DSS05	

1. Doel

1.1 Dit beleid stelt vast hoe testgegevens en testomgevingen moeten worden beheerd om onbedoelde blootstelling, datalekken of operationele verstoringen tijdens testactiviteiten te voorkomen.

1.2 Het waarborgt dat echte klantgegevens nooit onjuist worden gebruikt tijdens software- of systeemtests en dat testomgevingen logisch en technisch zijn gescheiden van productieomgevingen.

1.3 Dit beleid is opgesteld om mkb-organisaties te ondersteunen bij het voldoen aan de vereisten voor ISO/IEC 27001-certificering en toepasselijke wet- en regelgeving inzake gegevensbescherming, terwijl het praktisch en afdwingbaar blijft voor organisaties zonder eigen IT-team.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle testomgevingen (bijvoorbeeld stagingservers, sandboxomgevingen en ontwikkeltestomgevingen)

2.1.2 alle testgegevens, ongeacht of deze handmatig zijn aangemaakt, gegenereerd of afgeleid van productiegegevens

2.1.3 al het personeel dat betrokken is bij testactiviteiten, met inbegrip van werknemers, contractanten, freelancers en IT-dienstverleners

2.1.4 alle tests die gevolgen kunnen hebben voor publieksgerichte platforms, interne bedrijfssystemen of diensten van derden

2.2 Dit beleid omvat zowel technische omgevingen als processen die worden gebruikt ter ondersteuning van:

2.2.1 de ontwikkeling van websites, applicaties en tools

2.2.2 systeemupgrades, configuratietests en integratietests

2.2.3 geautomatiseerde en handmatige functionele tests of beveiligingstests

3. Doelstellingen

3.1 Het gebruik van echte, identificeerbare klantgegevens in tests voorkomen, tenzij deze zijn geanonimiseerd en uitdrukkelijk goedgekeurd.

3.2 Een strikte scheiding tussen test- en productieomgevingen handhaven om onbedoelde gegevensblootstelling of operationele verstoring te voorkomen.

3.3 Testsystemen en testgegevens beschermen tegen ongeautoriseerde toegang, onbedoelde openbaarmaking of hergebruik tussen omgevingen zonder passende beheersmaatregelen.

3.4 Voldoen aan relevante regelgeving inzake gegevensbescherming (bijvoorbeeld de AVG en NIS2) door te waarborgen dat alle testgegevens rechtmatig, behoorlijk en veilig worden verwerkt.

3.5 De gereedheid van de organisatie voor externe audits en ISO/IEC 27001-certificering ondersteunen door testpraktijken te documenteren en consistente waarborgen af te dwingen.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Draagt de eindverantwoordelijkheid voor de bescherming van testgegevens en de beveiliging van testsystemen.

4.1.2 Keurt elk gebruik van echte gegevens in tests goed nadat is vastgesteld dat passende waarborgen zijn getroffen (bijvoorbeeld anonimisering of gegevensmaskering).

4.1.3 Verifieert dat testactiviteiten naar behoren zijn gedocumenteerd en in overeenstemming zijn met dit beleid.

4.2 Projecteigenaar

4.2.1 Coördineert het ontwerp en de uitvoering van testprocessen.

4.2.2 Zorgt ervoor dat alle teamleden dit beleid begrijpen en naleven.

4.2.3 Bevestigt dat testsystemen veilig zijn geconfigureerd voordat het testen begint.

4.2.4 Meldt incidenten met betrekking tot testomgevingen of gegevenslekken aan de GM.

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

9. Vereisten voor herziening en actualisering

9.1 Geplande beoordelingen

9.1.1 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld door de Algemeen directeur (GM). Deze beoordeling waarborgt dat het beleid actueel blijft met betrekking tot:

9.1.1.1 wijzigingen in tools, platforms of omgevingen voor softwareontwikkeling

9.1.1.2 bijgewerkte wettelijke verplichtingen, met inbegrip van vereisten inzake gegevensbescherming of digitale weerbaarheid

9.1.1.3 mkb-certificering en auditgereedheid onder ISO/IEC 27001

9.2 Triggergebeurtenissen voor tussentijdse beoordeling

9.2.1 Aanvullende beoordelingen moeten plaatsvinden naar aanleiding van:

9.2.1.1 elk incident met gegevensblootstelling of compromittering in testomgevingen

9.2.1.2 het gebruik van echte gegevens in tests, ook indien deze zijn geanonimiseerd

9.2.1.3 de introductie van nieuwe testmethoden, systemen of leveranciers

9.2.1.4 regelgevende updates die gevolgen hebben voor de verwerking van gegevens tijdens tests

9.3 Wijzigingsbeheer en communicatie

9.3.1 De GM is verantwoordelijk voor:

9.3.1.1 het actualiseren van dit beleid en het documenteren van wijzigingen in de versiehistorie

9.3.1.2 het informeren van personeel, ontwikkelaars en relevante dienstverleners over updates

9.3.1.3 het bevestigen dat al het personeel dat betrokken is bij testen de meest recente regels begrijpt en toepast

9.3.1.4 het beschikbaar houden van een toegankelijke versie van het meest recente beleid voor beoordelings- en auditdoeleinden

9.4 Audit en documentatie

9.4.1 Registraties van alle beleidsbeoordelingen, goedkeuringen voor het gebruik van echte gegevens en motiveringen voor uitzonderingen moeten:

9.4.1.1 veilig worden bewaard voor auditdoeleinden

9.4.1.2 op verzoek beschikbaar zijn tijdens interne audits of audits door derden

9.4.1.3 jaarlijks worden beoordeeld om overeenstemming met de testpraktijken te waarborgen

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet in samenhang met de volgende mkb-beleidslijnen worden toegepast om beveiliging en naleving tijdens testactiviteiten te waarborgen:

10.1.1 P2S – Beleid inzake governance, rollen en verantwoordelijkheden: definieert wie verantwoordelijk is voor het toezicht op ontwikkeling, testen en verantwoordelijkheden inzake omgevingsscheiding.

10.1.2 P4S – Beleid inzake toegangsbeheer: regelt de toewijzing, het beheer en de intrekking van toegangsgegevens voor testsystemen.

10.1.3 P8S – Beleid inzake bewustwording en opleiding op het gebied van informatiebeveiliging: zorgt ervoor dat personeel de risico's van testgegevens, veilige verwerkingspraktijken en de juiste scheiding van omgevingen begrijpt.

10.1.4 P13S – Beleid inzake gegevensclassificatie en etikettering: ondersteunt een duidelijke classificatie van testgegevens en geeft richting aan strategieën voor anonimisering of gegevensmaskering.

10.1.5 P17S – Beleid inzake gegevensbescherming en privacy: sluit aan op AVG-verplichtingen, inclusief waarborgen voor de verwerking en opslag van persoonsgegevens, ook in niet-productieomgevingen.

10.1.6 P24S – Beleid inzake veilige ontwikkeling: biedt overkoepelende beveiligingsvereisten voor ontwikkelteams, waaronder het veilige gebruik van gegevens tijdens testfasen.

10.1.7 P30S – Incidentresponsbeleid (P30): beschrijft hoe moet worden gereageerd op inbreuken of problemen die in een testomgeving worden ontdekt of worden veroorzaakt door onjuiste verwerking van testgegevens.

10.2 Deze beleidslijnen vormen samen één samenhangend beveiligingskader ter ondersteuning van de integriteit van tests, gegevensminimalisatie en volledige afstemming op ISO/IEC 27001 binnen ontwikkel- en QA-activiteiten.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1 – Vereist risicobeoordeling en risicobehandeling, met inbegrip van testgerelateerde risico's.

11.1.2 Clausule 8.1 – Vereist planning en beheersing van operationele processen, met inbegrip van de inrichting van testomgevingen.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.28 – Vereist dat organisaties testgegevens beschermen en waarborgen dat deze geen gevoelige gegevens of productiegegevens bevatten.

11.2.2 Beheersmaatregel 8.29 – Vereist een duidelijke scheiding tussen ontwikkel-, test- en productieomgevingen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Omvat vereisten voor beheersmaatregelen bij ontwikkeling en testen.

11.3.2 SA-12 – Behandelt testgerelateerde risico's in de toeleveringsketen en beveiligingsevaluaties.

11.3.3 SC-32 – Vereist scheiding van omgevingen en bescherming van de vertrouwelijkheid en integriteit van testgegevens.

11.4 Algemene verordening gegevensbescherming (AVG) van de EU

11.4.1 Artikel 5(1)(c) – Vereist gegevensminimalisatie, waaronder het gebruik van uitsluitend noodzakelijke gegevens voor testdoeleinden.

11.4.2 Artikel 25 – Vereist gegevensbescherming door ontwerp, waaronder beheersmaatregelen voor testomgevingen.

11.4.3 Artikel 32 – Vereist veilige verwerking van persoonsgegevens in alle systemen, met inbegrip van niet-productieomgevingen.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(e), (h) – Vereist veilige ontwikkeling en systeemtests, met name waar digitale diensten blootstaan aan cyberrisico's.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Benadrukt het belang van digitale operationele weerbaarheid, waaronder het veilig testen van ICT-systemen door mkb-organisaties in de financiële sector.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: omvat testbeheersmaatregelen voor de validatie van nieuwe systemen en gegevensverwerking.

11.7.2 DSS05 – Manage Security Services: vereist test- en ontwikkelpraktijken die misbruik of blootstelling van bedrijfsgegevens voorkomen.