					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P29					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**

Afstemming op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	Relevant voor de veilige planning en beheersing van testgegevens en testomgevingen
ISO/IEC 27002:2022	Beheersmaatregelen 8.28–8.29	Omvat veilige testgegevens en de bescherming van testomgevingen
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Behandelt ontwikkelaarstesten en -evaluaties, bescherming van gegevens in rust en integriteit
AVG	Artikelen 5, 25, 32	Omvat gegevensminimalisatie, privacy by design en beveiliging van verwerking in testcontexten
NIS2	Artikel 21(2)(e), (h)	Houdt verband met veilige ontwikkel- en testpraktijken
DORA	Artikel 9	Betreft ICT-systemen en protocollen en de beveiliging van testgegevens
COBIT 2019	DSS05, BAI07	Behandelt het beheer van beveiligingsdiensten en wijzigingsacceptatie en -transitie

1. Doel

1.1. Dit beleid stelt verplichte eisen vast voor het beheer van testomgevingen en testgegevens om de beveiliging, vertrouwelijkheid en operationele integriteit gedurende de volledige levenscyclus van softwareontwikkeling en testen te waarborgen.

1.2. Dit beleid heeft tot doel ongeautoriseerde toegang, gegevenslekken en besmetting van productiesystemen te voorkomen als gevolg van onjuist beheerde testomgevingen of het gebruik van productiegegevens in tests.

1.3. Dit beleid verplicht tot veilige omgang met gegevens die voor tests worden gebruikt, hardening van testinfrastructuur en rolgebaseerde toegangsbeheersing, in overeenstemming met toepasselijke wettelijke, regelgevende en contractuele verplichtingen.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle testomgevingen, gegevens, tools en processen die binnen de organisatie worden gebruikt voor het testen van software, systemen, applicaties en infrastructuur.

2.2. Dit beleid omvat:

2.2.1. Testomgevingen die zijn ingericht on-premises, in de cloud of via platforms van derden

2.2.2. Testgegevens die worden gebruikt voor functionele tests, performancetests, regressietests en beveiligingstests

2.2.3. Handmatig, gescript of geautomatiseerd testen (bijvoorbeeld CI/CD-pijplijnen)

2.2.4. Al het personeel dat betrokken is bij testen, met inbegrip van interne teams, leveranciers en contractanten

2.3. Dit beleid is van toepassing ongeacht de criticaliteit van het systeem, het type applicatie of de vraag of ontwikkeling intern of uitbesteed plaatsvindt.

3. Doelstellingen

3.1. Het voorkomen van het gebruik van live-, gevoelige of gereguleerde gegevens (bijvoorbeeld persoonlijk identificeerbare informatie (PII), kaartgegevens) in testomgevingen, tenzij deze zijn geanonimiseerd of hiervoor specifiek goedkeuring is verleend.

3.2. Het waarborgen van volledige netwerk- en toegangsscheiding tussen test- en productieomgevingen om ongeautoriseerde toegang tot gegevens of besmetting van systemen te voorkomen.

3.3. Het verplicht stellen van encryptie, datamasking of het genereren van synthetische gegevens wanneer representatieve gegevens nodig zijn voor testdoeleinden.

3.4. Het verminderen van de kans op non-compliance, blootstelling van klantgegevens of operationele verstoringen als gevolg van onveilige testgegevens of testomgevingen.

3.5. Het afstemmen van de omgang met testgegevens op industrienormen (ISO, NIST, COBIT) en regelgeving zoals de AVG, NIS2 en DORA.

4. Rollen en verantwoordelijkheden

4.1. Chief Information Security Officer (CISO)

4.1.1. Is eigenaar van dit beleid en ziet toe op de implementatie van technische en administratieve beheersmaatregelen voor testgegevens en testomgevingen.

4.1.2. Keurt het gebruik van echte of gevoelige gegevens voor tests goed op basis van een passende onderbouwing en compenserende beheersmaatregelen.

4.2. QA-/Testleads

4.2.1. Coördineren de testplanning en waarborgen dat alle testactiviteiten voldoen aan de eisen van dit beleid.

4.2.2. Valideren de juiste scheiding, toegang en gegevensvoorbereiding voor elke testfase.

[... 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 actualisatie

9.1. Dit beleid moet jaarlijks worden herzien en waar nodig worden bijgewerkt om rekening te houden met:

9.1.1. Wijzigingen in wettelijke en regelgevende vereisten (bijvoorbeeld AVG, DORA, NIS2)

9.1.2. Ingebruikname van nieuwe testtools, platforms of automatiseringspijplijnen

9.1.3. Bevindingen uit interne audits of aanbevelingen naar aanleiding van incidenten

9.1.4. Uitbreiding van ontwikkel- of QA-processen die de omgang met testgegevens of het gebruik van omgevingen wijzigen

9.2. De CISO is verantwoordelijk voor het initiëren van de herziening in samenwerking met:

9.2.1. QA-/Testleads

9.2.2. DevOps- en infrastructuurmanagers

9.2.3. Applicatieontwikkelingsteams

9.2.4. De Functionaris voor Gegevensbescherming (FG) en een juridisch adviseur

9.3. Alle revisies moeten:

9.3.1. Onder versiebeheer staan en worden opgeslagen in de centrale documentrepository

9.3.2. Via formele kanalen aan betrokken medewerkers worden gecommuniceerd (bijvoorbeeld ISMS-meldingen, teambriefings)

9.3.3. Worden gekoppeld aan actualisaties van gerelateerde technische standaarden, beheersmaatregelen en standaardwerkinstructies

9.4. Tussentijdse herzieningen op basis van triggers moeten onmiddellijk worden uitgevoerd na:

9.4.1. Een gegevenslek of inbreuk met betrekking tot testomgevingen

9.4.2. Een auditafwijking met betrekking tot de omgang met testgegevens

9.4.3. Significante wijzigingen in wettelijke verplichtingen of IT-architectuur

10. Gerelateerde beleidslijnen en samenhang

10.1. Dit beleid is nauw verbonden met de volgende beleidslijnen om een veilige en conforme omgang met testgegevens en testomgevingen te waarborgen:

10.1.1. P1 – Informatiebeveiligingsbeleid: stelt de overkoepelende beveiligingsprincipes vast die gelden voor de bescherming van testgegevens en het beheer van omgevingen.

10.1.2. P5 – Wijzigingsbeheerbeleid: is van toepassing op het creëren, actualiseren en buiten gebruik stellen van testomgevingen en uitrolpijplijnen.

10.1.3. P13 – Beleid inzake gegevensclassificatie en etikettering: biedt richting voor de selectie van testgegevens en het afdwingen van beheersmaatregelen op basis van gevoeligheid.

10.1.4. P14 – Gegevensbewarings- en vernietigingsbeleid: definieert bewaartermijnen en vereisten voor veilige vernietiging van testdatasets.

10.1.5. P15 – Beleid inzake back-up en herstel: stelt back-uppraktijken en validatie van herstel voor testomgevingen verplicht.

10.1.6. P18 – Beleid inzake cryptografische beheersmaatregelen: specificeert verplichte encryptiestandaarden voor gegevens in rust en gegevens tijdens transport binnen testplatforms.

10.1.7. P22 – Logging- en monitoringbeleid: regelt zichtbaarheid en detectie van afwijkingen voor activiteiten in testomgevingen.

10.1.8. P30 – Incidentresponsbeleid: definieert escalatie en remediatie voor inbreuken of incidenten met betrekking tot testsystemen.

10.1.9. P33 – Beleid inzake audit- en nalevingsmonitoring: maakt validatie van naleving van beleid en continue assurance mogelijk.

11. Referentienormen en -raamwerken

11.1. Dit beleid is afgestemd op mondiale normen voor cyberbeveiliging en regelgevende kaders die een veilige omgang met testgegevens en bescherming van niet-productieomgevingen vereisen.

11.2. ISO/IEC 27001:

11.2.1. Clausule 8.1 - Verplicht veilige planning en beheersing van testgegevens en testomgevingen.

11.3. ISO/IEC 27002:2022 – Beheersmaatregelen 8.28–8.29:

11.3.1. Annex A-beheersmaatregel 8.28 – Veilige testgegevens: vereist bescherming van testgegevens die worden gebruikt in ontwikkel- en testfasen door middel van anonimisering, datamasking of synthetische generatie.

11.3.2. Annex A-beheersmaatregel 8.29 – Bescherming van testomgevingen: vereist scheiding van productie, toegangsbeheersmaatregelen en hardening van omgevingen voor testsystemen.

11.3.3. Deze beheersmaatregelen beschrijven vereisten voor het veilig beheren van gegevens die tijdens tests worden gebruikt en voor het beschermen van niet-productiesystemen tegen misbruik, compromittering of besmetting.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Ontwikkelaarstesten en -evaluatie: stelt verwachtingen vast voor veilige, herhaalbare testprocedures met passende gegevensbeheersmaatregelen.

11.4.2. SC-28 – Bescherming van informatie in rust: sluit aan op encryptie van testgegevens die zijn opgeslagen in niet-productiesystemen.

11.4.3. SC-32 – Integriteit van informatie: ondersteunt gegevensvalidatie, voorkoming van corruptie en invoer-/uitvoercontroles tijdens tests.

11.5. AVG (2016/679):

11.5.1. Artikel 5 – Gegevensminimalisatie: verbiedt onnodig gebruik van persoonsgegevens in tests.

11.5.2. Artikel 25 – Privacy by design: vereist dat technieken voor gegevensbescherming vanaf het begin van de ontwikkel- en testcyclus worden toegepast.

11.5.3. Artikel 32 – Beveiliging van verwerking: verplicht waarborgen voor testomgevingen die persoonsgegevens of gevoelige gegevens verwerken.

11.6. NIS2-richtlijn (2022/2555):

11.6.1. Artikel 21(2)(e, h): vereist veilige processen voor softwareontwikkeling en testen, met nadruk op bescherming tegen ongeautoriseerde toegang en gegevenslekken.

11.7. DORA (2022/2554):

11.7.1. Artikel 9 – ICT-systemen en protocollen: vereist dat testprocessen de operationele weerbaarheid ondersteunen en operationele gegevens beschermen tegen compromittering of ongeautoriseerde openbaarmaking.

11.8. COBIT 2019:

11.8.1. DSS05 – Manage Security Services: ondersteunt de handhaving van beveiligingsbeleid in alle omgevingen, inclusief niet-productieomgevingen.

11.8.2. BAI07 – Manage Change Acceptance and Transition: omvat het formele transitieproces van testen naar productie, inclusief beheersmaatregelen voor gegevens en omgevingen.