					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P29S					Dokumenttitel: **Politik for testdata og testmiljøer**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 8	
ISO/IEC 27002:2022	Kontrol 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
EU GDPR	Artikel 5(1)(c), 25, 32	
EU NIS2	Artikel 21(2)(e), (h)	
EU DORA	Artikel 9	
COBIT 2019	BAI07, DSS05	

1. Formål

1.1 Denne politik fastsætter, hvordan testdata og testmiljøer skal styres for at forhindre utilsigtet eksponering, brud på persondatasikkerheden eller driftsforstyrrelser under testaktiviteter.

1.2 Den sikrer, at reelle kundedata aldrig anvendes uretmæssigt under software- eller systemtest, og at testmiljøer er logisk og teknisk adskilt fra produktionssystemer.

1.3 Politikken er udformet til at hjælpe SMV'er med at opfylde kravene til ISO/IEC 27001-certificering og relevant databeskyttelseslovgivning, samtidig med at den forbliver praktisk og håndhævelig for organisationer uden et dedikeret it-team.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle testmiljøer (f.eks. stagingmiljøer, sandbox-miljøer og udviklingstestmiljøer)

2.1.2 Alle testdata, uanset om de er manuelt oprettet, genereret eller afledt af driftsdata

2.1.3 Alt personale, der deltager i testaktiviteter, herunder medarbejdere, kontrahenter, freelancere og it-leverandører

2.1.4 Enhver test, der kan påvirke kundevendte platforme, interne forretningssystemer eller tredjepartstjenester

2.2 Den omfatter både tekniske miljøer og processer, der anvendes til at understøtte:

2.2.1 Udvikling af websteder, applikationer og værktøjer

2.2.2 Systemopgraderinger, konfigurationstest og integrationstest

2.2.3 Automatiserede og manuelle funktionstest eller sikkerhedstest

3. Mål

3.1 Forhindre brug af reelle, identificerbare kundedata i test, medmindre de er anonymiseret og udtrykkeligt godkendt.

3.2 Opretholde en streng adskillelse mellem test- og produktionssystemer for at undgå utilsigtet dataeksponering eller driftsmæssig påvirkning.

3.3 Beskytte testsystemer og testdata mod uautoriseret adgang, utilsigtet videregivelse eller genbrug på tværs af miljøer uden passende kontroller.

3.4 Overholde relevante databeskyttelseskrav (f.eks. GDPR og NIS2) ved at sikre, at alle testdata behandles lovligt, rimeligt og sikkert.

3.5 Understøtte organisationens revisionsberedskab ved eksterne revisioner og ISO/IEC 27001-certificering ved at dokumentere testpraksis og håndhæve ensartede sikkerhedsforanstaltninger.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for beskyttelse af testdata og sikkerheden i testsystemer.

4.1.2 Godkender enhver brug af reelle data i test efter at have bekræftet, at passende sikkerhedsforanstaltninger er etableret (f.eks. anonymisering eller datamaskering).

4.1.3 Verificerer, at testaktiviteter dokumenteres korrekt og er i overensstemmelse med denne politik.

4.2 Projektejer

4.2.1 Koordinerer udformning og gennemførelse af testprocesser.

4.2.2 Sikrer, at alle teammedlemmer forstår og efterlever denne politik.

4.2.3 Bekræfter, at testsystemer er konfigureret sikkert, før testen påbegyndes.

4.2.4 Rapporterer alle hændelser vedrørende testmiljøer eller datalækager til direktøren.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Planlagte gennemgange

9.1.1 Denne politik skal gennemgås mindst én gang om året af direktøren (GM). Gennemgangen skal sikre, at politikken fortsat er ajour med:

9.1.1.1 Ændringer i værktøjer, platforme eller miljøer til softwareudvikling

9.1.1.2 Opdaterede juridiske forpligtelser, herunder krav til databeskyttelse eller digital operationel robusthed

9.1.1.3 SMV'ers certificerings- og revisionsberedskab efter ISO/IEC 27001

9.2 Udløsende forhold for ekstraordinær gennemgang

9.2.1 Yderligere gennemgange skal gennemføres efter:

9.2.1.1 Enhver hændelse, der omfatter dataeksponering eller kompromittering i testmiljøer

9.2.1.2 Brug af reelle data i test, selv hvis de er anonymiserede

9.2.1.3 Indførelse af nye testmetoder, systemer eller leverandører

9.2.1.4 Regulatoriske opdateringer, der påvirker håndteringen af data under test

9.3 Ændringsstyring og kommunikation

9.3.1 Direktøren er ansvarlig for:

9.3.1.1 At opdatere denne politik og dokumentere alle ændringer i versionshistorikken

9.3.1.2 At underrette medarbejdere, udviklere og relevante tjenesteudbydere om opdateringer

9.3.1.3 At bekræfte, at alt testrelateret personale forstår og anvender de seneste krav

9.3.1.4 At opretholde en tilgængelig version af den seneste politik til brug for gennemgang og revision

9.4 Revision og dokumentation

9.4.1 Registreringer af alle politikgennemgange, godkendelser af brug af reelle data og begrundelser for undtagelser skal:

9.4.1.1 Opbevares sikkert til revisionsformål

9.4.1.2 Være tilgængelige efter anmodning ved intern revision eller revision udført af tredjeparter

9.4.1.3 Gennemgås årligt for at sikre overensstemmelse med testpraksis

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal anvendes i sammenhæng med følgende SME-politikker for at opretholde sikkerhed og efterlevelse under test:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Definerer, hvem der er ansvarlig for tilsyn med udvikling, test og ansvar for adskillelse af systemer.

10.1.2 P4S – Politik for adgangskontrol: Regulerer tildeling, styring og fjernelse af legitimationsoplysninger til adgang til testsystemer.

10.1.3 P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at medarbejdere forstår risici ved testdata, praksis for sikker håndtering og korrekt adskillelse af miljøer.

10.1.4 P13S – Politik for dataklassificering og mærkning: Understøtter tydelig klassificering af testdata og vejleder om strategier for anonymisering eller datamaskering.

10.1.5 P17S – Databeskyttelses- og privatlivspolitik: Sikrer sammenhæng med GDPR-forpligtelser, herunder sikkerhedsforanstaltninger ved behandling og lagring af personoplysninger, også i ikke-produktionsmiljøer.

10.1.6 P24S – Politik for sikker udvikling: Fastlægger de overordnede sikkerhedsforventninger til udviklingsteams, herunder sikker brug af data i testfaser.

10.1.7 P30S – Politik for hændelseshåndtering: Beskriver, hvordan der skal reageres på ethvert brud eller problem, der opdages i et testmiljø eller skyldes forkert håndtering af testdata.

10.2 Disse politikker udgør en samlet styringsramme for sikkerhed, som understøtter testintegritet, dataminimering og fuld overensstemmelse med ISO/IEC 27001 på tværs af udviklings- og QA-aktiviteter.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Kræver risikovurdering og risikobehandling, herunder risici relateret til test.

11.1.2 Klausul 8.1 – Kræver operationel planlægning og styring, herunder etablering af testmiljøer.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.28 – Kræver, at organisationer beskytter testdata og sikrer, at de ikke indeholder følsomme data eller driftsdata fra produktionsmiljøet.

11.2.2 Kontrol 8.29 – Kræver klar adskillelse mellem udviklings-, test- og produktionsmiljøer.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Omfatter krav til kontroller for udvikling og test.

11.3.2 SA-12 – Omhandler risici ved test i forsyningskæden og sikkerhedsevalueringer.

11.3.3 SC-32 – Kræver adskillelse af miljøer og beskyttelse af testdatas fortrolighed og integritet.

11.4 Databeskyttelsesforordningen (GDPR)

11.4.1 Artikel 5(1)(c) – Kræver dataminimering, herunder at kun nødvendige data anvendes til test.

11.4.2 Artikel 25 – Kræver databeskyttelse gennem design, hvilket omfatter kontroller for testmiljøer.

11.4.3 Artikel 32 – Kræver sikker behandling af personoplysninger i alle systemer, herunder ikke-produktionsmiljøer.

11.5 NIS2-direktivet (EU) 2022/2555

11.5.1 Artikel 21(2)(e, h) – Kræver sikker udvikling og systemtest, særligt hvor digitale tjenester er eksponeret for cyberrisici.

11.6 DORA-forordningen (EU) 2022/2554

11.6.1 Artikel 9 – Fremhæver betydningen af digital operationel robusthed, herunder sikker test af IKT-systemer udført af SMV'er i den finansielle sektor.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: Omfatter testkontroller til validering af nye systemer og datahåndtering.

11.7.2 DSS05 – Manage Security Services: Kræver test- og udviklingspraksis, der forhindrer misbrug eller eksponering af forretningsdata.