					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P29					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 regulering

Standard/regulering	Bestemmelse/artikel	Kommentar
ISO/IEC 27001:2022	Clause 8	Relevant for sikker planlægning og styring af testdata og testmiljøer
ISO/IEC 27002:2022	Controls 8.28–8.29	Omfatter sikker håndtering af testdata og beskyttelse af testmiljøer
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Omhandler udviklertest/-evaluering, beskyttelse af data i hvile og dataintegritet
EU GDPR	Articles 5, 25, 32	Omfatter dataminimering, databeskyttelse gennem design og behandlingssikkerhed i testkontekster
EU NIS2	Article 21(2)(e), (h)	Relaterer sig til praksis for sikker udvikling og test
EU DORA	Article 9	Vedrører IKT-systemer og -protokoller samt sikkerhed for testdata
COBIT 2019	DSS05, BAI07	Omhandler styring af sikkerhedstjenester og ændringsaccept/-overgang

1. Formål

1.1. Denne politik fastsætter de obligatoriske krav til styring af testmiljøer og testdata for at sikre sikkerhed, fortrolighed og driftsmæssig integritet gennem hele softwareudviklings- og testlivscyklussen.

1.2. Formålet er at forhindre uautoriseret adgang, datalækage og kontaminering af produktionssystemer som følge af utilstrækkeligt styrede testmiljøer eller anvendelse af produktionsdata i test.

1.3. Politikken kræver sikker håndtering af data, der anvendes til test, hærdning af testinfrastruktur og rollebaserede adgangskontroller samt tilpasning til gældende regulatoriske og kontraktuelle forpligtelser.

2. Omfang

2.1. Denne politik gælder for alle testmiljøer, data, værktøjer og processer, der anvendes til test af software, systemer, applikationer og infrastruktur i hele organisationen.

2.2. Den omfatter:

2.2.1. Testmiljøer etableret på lokal infrastruktur, i cloudtjenester eller via tredjepartsplatforme

2.2.2. Testdata anvendt i funktionstest, performancetest, regressionstest og sikkerhedstest

2.2.3. Manuel, scriptbaseret eller automatiseret test (f.eks. CI/CD-pipelines)

2.2.4. Alt personale, der deltager i test, herunder interne teams, leverandører og konsulenter

2.3. Politikken gælder uanset systemets kritikalitet, applikationstype eller om udviklingen udføres internt eller er outsourcet.

3. Mål

3.1. At forhindre anvendelse af live-, følsomme eller regulerede data (f.eks. personhenførbare oplysninger (PII), kortindehaverdata) i testmiljøer, medmindre dataene er anonymiserede eller specifikt godkendt.

3.2. At sikre fuldstændig netværksmæssig og adgangsmæssig adskillelse mellem test- og produktionsmiljøer for at undgå uautoriseret dataadgang eller kontaminering af systemer.

3.3. At kræve kryptering, datamaskering eller generering af syntetiske data, når repræsentative data er nødvendige til testformål.

3.4. At reducere sandsynligheden for manglende efterlevelse, eksponering af kundedata eller driftsforstyrrelser som følge af usikre testdata eller testmiljøer.

3.5. At bringe håndtering af testdata i overensstemmelse med branchestandarder (ISO, NIST, COBIT) og regler som GDPR, NIS2 og DORA.

4. Roller og ansvar

4.1. Chief Information Security Officer (CISO)

4.1.1. Ejer denne politik og håndhæver tekniske og administrative sikkerhedsforanstaltninger for testdata og testmiljøer.

4.1.2. Godkender anvendelse af produktionsdata eller følsomme data i test med passende begrundelse og kompenserende kontroller.

4.2. QA-/testansvarlige

4.2.1. Koordinerer testplanlægning og sikrer, at alle testaktiviteter overholder kravene i denne politik.

4.2.2. Validerer korrekt adskillelse, adgang og klargøring af data for hver testfase.

[... 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. Denne politik skal gennemgås årligt og opdateres efter behov for at afspejle:

9.1.1. Ændringer i regulatoriske krav (f.eks. GDPR, DORA, NIS2)

9.1.2. Indførelse af nye testværktøjer, platforme eller automatiseringspipelines

9.1.3. Revisionsresultater fra intern revision eller anbefalinger efter hændelser

9.1.4. Udvidelse af udviklings- eller QA-processer, der ændrer håndtering af testdata eller anvendelse af testmiljøer

9.2. CISO er ansvarlig for at iværksætte gennemgangen i samarbejde med:

9.2.1. QA-/testansvarlige

9.2.2. DevOps- og infrastrukturansvarlige

9.2.3. Applikationsudviklingsteams

9.2.4. Databeskyttelsesrådgiver (DPO) og juridisk rådgiver

9.3. Alle revisioner af politikken skal være:

9.3.1. Versionsstyret og opbevaret i det centrale dokumentrepository

9.3.2. Kommunikeret til berørt personale gennem formelle kanaler (f.eks. ISMS-underretninger, teambriefinger)

9.3.3. Koblet til opdateringer i tilhørende tekniske standarder, kontroller og driftsprocedurer

9.4. Ekstraordinære gennemgange udløst af hændelser skal gennemføres straks efter enhver:

9.4.1. Datalækage eller sikkerhedsbrud, der involverer testmiljøer

9.4.2. Afvigelse konstateret ved revision relateret til håndtering af testdata

9.4.3. Væsentlig ændring i juridiske forpligtelser eller IT-arkitektur

10. Relaterede politikker og sammenhænge

10.1. Denne politik er tæt integreret med følgende politikker for at sikre sikker og compliant håndtering af testdata og testmiljøer:

10.1.1. P1 – Informationssikkerhedspolitik: Fastlægger overordnede sikkerhedsprincipper, der styrer beskyttelse af testdata og styring af testmiljøer.

10.1.2. P5 – Politik for ændringsstyring: Gælder for etablering, opdatering og udfasning af testmiljøer og udrulningspipelines.

10.1.3. P13 – Politik for dataklassificering og mærkning: Styrer valg af testdata og håndhævelse af kontroller baseret på følsomhed.

10.1.4. P14 – Politik for dataopbevaring og bortskaffelse: Fastlægger opbevaringsfrister og krav til sikker bortskaffelse af testdatasæt.

10.1.5. P15 – Politik for backup og gendannelse: Kræver sikkerhedskopieringspraksis og validering af gendannelse for testmiljøer.

10.1.6. P18 – Politik for kryptografiske kontroller: Specificerer obligatoriske krypteringsstandarder for data i hvile og data under overførsel i testplatforme.

10.1.7. P22 – Lognings- og overvågningspolitik: Regulerer synlighed og anomalidetektion for aktiviteter i testmiljøer.

10.1.8. P30 – Politik for hændelseshåndtering: Definerer eskalering og afhjælpning ved brud eller hændelser, der involverer testsystemer.

10.1.9. P33 – Politik for revisions- og efterlevelsesovervågning: Muliggør validering af overholdelse af politikker og løbende sikkerhed.

11. Referencestandarder og rammeværker

11.1. Denne politik er tilpasset globale cybersikkerhedsstandarder og regulatoriske rammer, der kræver sikker håndtering af testdata og beskyttelse af ikke-produktionsmiljøer.

11.2. ISO/IEC 27001:

11.2.1. Clause 8.1 - Kræver sikker planlægning og styring af testdata og testmiljøer.

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

11.3.1. Annex A Control 8.28 – Secure Test Data: Kræver beskyttelse af testdata, der anvendes i udviklings- og testfaser, gennem anonymisering, maskering eller generering af syntetiske data.

11.3.2. Annex A Control 8.29 – Protection of Test Environments: Kræver adskillelse fra produktion, adgangskontroller og hærdning af testmiljøer.

11.3.3. Disse kontroller beskriver krav til sikker styring af data, der anvendes under test, og til beskyttelse af ikke-produktionssystemer mod misbrug, kompromittering eller kontaminering.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Developer Testing and Evaluation: Fastlægger forventninger til sikre, gentagelige testprocedurer med passende datakontroller.

11.4.2. SC-28 – Protection of Information at Rest: Er i overensstemmelse med kryptering af testdata, der opbevares i ikke-produktionssystemer.

11.4.3. SC-32 – Information Integrity: Understøtter datavalidering, forebyggelse af datakorruption og input-/outputkontroller under test.

11.5. EU GDPR (2016/679):

11.5.1. Article 5 – Data Minimization: Forbyder unødvendig brug af personoplysninger i test.

11.5.2. Article 25 – Privacy by Design: Kræver, at databeskyttelsesteknikker anvendes fra starten af udviklings- og testcyklussen.

11.5.3. Article 32 – Security of Processing: Kræver sikkerhedsforanstaltninger for testmiljøer, der håndterer personoplysninger eller følsomme data.

11.6. EU NIS2-direktivet (2022/2555):

11.6.1. Article 21(2)(e, h): Kræver sikre processer for softwareudvikling og test med vægt på beskyttelse mod uautoriseret adgang og datalækage.

11.7. EU DORA (2022/2554):

11.7.1. Article 9 – ICT Systems and Protocols: Kræver, at testprocesser understøtter robusthed og beskytter driftsdata mod kompromittering eller uautoriseret videregivelse.

11.8. COBIT 2019:

11.8.1. DSS05 – Styring af sikkerhedstjenester: Understøtter håndhævelse af sikkerhedspolitikker på tværs af alle miljøer, herunder ikke-produktion.

11.8.2. BAI07 – Manage Change Acceptance and Transition: Omfatter den formelle overgangsproces fra test til produktion, herunder data- og miljøkontroller.