					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P29					Dokumenttitel: **Policy för testdata och testmiljöer**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassad till standarder och regelverk

Standard/förordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Relevant för säker planering och styrning av testdata och testmiljöer
ISO/IEC 27002:2022	Kontroller 8.28–8.29	Omfattar säker testdata och skydd av testmiljöer
NIST SP 800-53 Rev. 5	SA-11, SC-28, SC-32	Omfattar utvecklartestning och utvärdering, skydd av data i vila samt informationsintegritet
EU:s dataskyddsförordning (GDPR)	Artiklarna 5, 25, 32	Omfattar uppgiftsminimering, inbyggt dataskydd och säkerhet i behandlingen i testkontexter
EU:s NIS2-direktiv	Artikel 21.2 e, h	Avser säker utvecklings- och testpraxis
EU:s DORA-förordning	Artikel 9	Avser IKT-system, protokoll och säkerhet för testdata
COBIT 2019	DSS05, BAI07	Omfattar hantering av säkerhetstjänster samt godkännande och övergång vid ändringar

1. Syfte

1.1. Denna policy fastställer obligatoriska krav för hantering av testmiljöer och testdata för att säkerställa säkerhet, konfidentialitet och operativ integritet genom hela livscykeln för programvaruutveckling och testning.

1.2. Policyn syftar till att förhindra obehörig åtkomst, dataläckage och påverkan på produktionssystem till följd av bristfälligt hanterade testmiljöer eller användning av verkliga data i testning.

1.3. Policyn kräver säker hantering av data som används vid testning, härdning av testinfrastruktur och rollbaserad åtkomstkontroll, i enlighet med tillämpliga regulatoriska krav och avtalskrav.

2. Omfattning

2.1. Denna policy gäller för alla testmiljöer, data, verktyg och processer som används för testning av programvara, system, applikationer och infrastruktur i hela organisationen.

2.2. Policyn omfattar:

2.2.1. Testmiljöer som tillhandahålls lokalt, i molnmiljö eller via tredjepartsplattformar

2.2.2. Testdata som används vid funktionstestning, prestandatestning, regressionstestning och säkerhetstestning

2.2.3. Manuell, skriptbaserad eller automatiserad testning (t.ex. CI/CD-pipelines)

2.2.4. All personal som deltar i testning, inklusive interna team, leverantörer, entreprenörer och tredjepartsleverantörer

2.3. Policyn gäller oavsett systemets kritikalitet, applikationstyp eller om utvecklingen sker internt eller är outsourcad.

3. Mål

3.1. Att förhindra användning av aktiva, känsliga eller reglerade data (t.ex. PII, kortinnehavardata) i testmiljöer om de inte har anonymiserats eller särskilt godkänts.

3.2. Att säkerställa fullständig nätverksmässig och behörighetsmässig åtskillnad mellan test- och produktionsmiljöer för att undvika obehörig dataåtkomst eller påverkan på system.

3.3. Att kräva kryptering, datamaskering eller generering av syntetiska data när representativa data behövs för teständamål.

3.4. Att minska sannolikheten för bristande regelefterlevnad, exponering av kunddata eller operativa störningar till följd av osäker testdata eller osäkra testmiljöer.

3.5. Att anpassa hanteringen av testdata till branschstandarder (ISO, NIST, COBIT) och regelverk såsom GDPR, NIS2 och DORA.

4. Roller och ansvar

4.1. Chief Information Security Officer (CISO)

4.1.1. Ansvarar för denna policy och säkerställer tekniska och administrativa skyddsåtgärder för testdata och testmiljöer.

4.1.2. Godkänner användning av verkliga eller känsliga data i testning när det finns lämplig motivering och kompenserande kontroller.

4.2. QA-/testansvariga

4.2.1. Samordnar testplanering och säkerställer att all testverksamhet följer kraven i denna policy.

4.2.2. Validerar korrekt åtskillnad, åtkomst och databeredning för varje testfas.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1. Denna policy ska granskas årligen och uppdateras vid behov för att återspegla:

9.1.1. Förändringar i regulatoriska krav (t.ex. GDPR, DORA, NIS2)

9.1.2. Införande av nya testverktyg, plattformar eller automatiseringspipelines

9.1.3. Revisionsiakttagelser från internrevision eller rekommendationer efter incidenter

9.1.4. Utökning av utvecklings- eller QA-processer som förändrar hanteringen av testdata eller användningen av testmiljöer

9.2. CISO ansvarar för att initiera granskningen i samarbete med:

9.2.1. QA-/testansvariga

9.2.2. DevOps- och infrastrukturansvariga

9.2.3. Applikationsutvecklingsteam

9.2.4. Dataskyddsombudet (DPO) och juridisk rådgivare

9.3. Alla revideringar ska:

9.3.1. Versionshanteras och lagras i det centrala dokumentarkivet

9.3.2. Kommuniceras till berörd personal genom formella kanaler (t.ex. ISMS-aviseringar, teamgenomgångar)

9.3.3. Kopplas till uppdateringar i tillhörande tekniska standarder, kontroller och driftrutiner

9.4. Omedelbara mellanliggande granskningar ska genomföras efter varje:

9.4.1. Dataläckage eller incident som rör testmiljöer

9.4.2. Revisionsavvikelse relaterad till hantering av testdata

9.4.3. Betydande förändring i rättsliga krav eller IT-arkitektur

10. Relaterade policyer och kopplingar

10.1. Denna policy är nära integrerad med följande policyer för att säkerställa säker och regelriktig hantering av testdata och testmiljöer:

10.1.1. P1 – Informationssäkerhetspolicy: Fastställer övergripande säkerhetsprinciper som styr skydd av testdata och hantering av testmiljöer.

10.1.2. P5 – Ändringshanteringspolicy: Gäller för etablering, uppdatering och avveckling av testmiljöer samt driftsättningspipelines.

10.1.3. P13 – Policy för dataklassificering och märkning: Vägleder val av testdata och tillämpning av kontroller utifrån känslighetsnivå.

10.1.4. P14 – Policy för databevarande och bortskaffande: Fastställer tidsramar för bevarande och krav på säker avveckling av testdataset.

10.1.5. P15 – Policy för säkerhetskopiering och återställning: Kräver säkerhetskopieringsrutiner och validering av återställning för testmiljöer.

10.1.6. P18 – Policy för kryptografiska kontroller: Anger obligatoriska krypteringsstandarder för data i vila och data under överföring inom testplattformar.

10.1.7. P22 – Loggnings- och övervakningspolicy: Reglerar synlighet och anomalidetektering för aktiviteter i testmiljöer.

10.1.8. P30 – Policy för incidenthantering: Fastställer eskalering och åtgärdande vid överträdelser eller incidenter som rör testsystem.

10.1.9. P33 – Policy för revisions- och efterlevnadsövervakning: Möjliggör validering av policyefterlevnad och kontinuerlig uppföljning.

11. Referensstandarder och ramverk

11.1. Denna policy är anpassad till globala cybersäkerhetsstandarder och regulatoriska ramverk som kräver säker hantering av testdata och skydd av miljöer utanför produktion.

11.2. ISO/IEC 27001:

11.2.1. Klausul 8.1 - Kräver säker planering och styrning av testdata och testmiljöer.

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

11.3.1. Bilaga A kontroll 8.28 – Säker testdata: Kräver att testdata som används i utvecklings- och testfaser skyddas genom anonymisering, datamaskering eller syntetisk generering.

11.3.2. Bilaga A kontroll 8.29 – Skydd av testmiljöer: Kräver åtskillnad från produktion, åtkomstkontroller och härdning av miljöer för testsystem.

11.3.3. Dessa kontroller beskriver krav för säker hantering av data som används under testning och för att skydda system utanför produktion mot felaktig användning, kompromettering eller påverkan.

11.4. NIST SP 800-53 Rev. 5:

11.4.1. SA-11 – Utvecklartestning och utvärdering: Fastställer förväntningar på säkra och repeterbara testförfaranden med lämpliga datakontroller.

11.4.2. SC-28 – Skydd av information i vila: Överensstämmer med kryptering av testdata som lagras i system utanför produktion.

11.4.3. SC-32 – Informationsintegritet: Stödjer datavalidering, förebyggande av korruption samt in- och utkontroller under testning.

11.5. EU:s dataskyddsförordning (GDPR):

11.5.1. Artikel 5 – Uppgiftsminimering: Förbjuder onödig användning av personuppgifter i testning.

11.5.2. Artikel 25 – Inbyggt dataskydd: Kräver att dataskyddstekniker tillämpas från början av utvecklings- och testcykeln.

11.5.3. Artikel 32 – Säkerhet i behandlingen: Kräver skyddsåtgärder för testmiljöer som hanterar personuppgifter eller känsliga data.

11.6. EU:s NIS2-direktiv (2022/2555):

11.6.1. Artikel 21(2)(e, h): Kräver säkra processer för programvaruutveckling och testning, med fokus på skydd mot obehörig åtkomst och dataläckage.

11.7. EU:s DORA-förordning (2022/2554):

11.7.1. Artikel 9 – IKT-system och protokoll: Kräver att testprocesser stöder resiliens och skyddar operativa data mot kompromettering eller obehörigt röjande.

11.8. COBIT 2019:

11.8.1. DSS05 – Manage Security Services: Stödjer tillämpning av säkerhetspolicyer i alla miljöer, inklusive icke-produktionsmiljöer.

11.8.2. BAI07 – Manage Change Acceptance and Transition: Omfattar den formella övergångsprocessen från test till produktion, inklusive kontroller för data och miljöer.