					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P29S					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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 8	
ISO/IEC 27002:2022	Kontroller 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
EU:s GDPR	Artiklar 5.1 c, 25, 32	
EU:s NIS2-direktiv	Artikel 21.2 e, h	
EU:s DORA-förordning	Artikel 9	
COBIT 2019	BAI07, DSS05	

1. Syfte

1.1 Denna policy fastställer hur testdata och testmiljöer ska hanteras för att förhindra oavsiktlig exponering, personuppgiftsincidenter eller driftstörningar under testaktiviteter.

1.2 Den säkerställer att verkliga kunduppgifter aldrig används otillbörligt vid programvaru- eller systemtestning och att testmiljöer är logiskt och tekniskt separerade från produktionssystem.

1.3 Policyn är utformad för att hjälpa små och medelstora företag att uppfylla kraven för ISO/IEC 27001-certifiering och tillämplig dataskyddslagstiftning, samtidigt som den förblir praktiskt tillämpbar och möjlig att efterleva för organisationer utan ett dedikerat IT-team.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla testmiljöer (t.ex. stagingservrar, sandboxmiljöer och testbäddar för utveckling)

2.1.2 All testdata, oavsett om den skapas manuellt, genereras eller härleds från produktionsdata

2.1.3 All personal som deltar i testaktiviteter, inklusive anställda, konsulter, tredjepartsleverantörer, frilansare och IT-leverantörer

2.1.4 All testning som kan påverka kundvända plattformar, interna verksamhetsapplikationer eller tredjepartstjänster

2.2 Den omfattar både tekniska miljöer och processer som används för att stödja:

2.2.1 Utveckling av webbplatser, applikationer och verktyg

2.2.2 Systemuppgraderingar, konfigurationstestning och integrationstestning

2.2.3 Automatiserade och manuella funktionstester eller säkerhetstester

3. Mål

3.1 Förhindra användning av verkliga, identifierbara kunduppgifter i testning om de inte har anonymiserats och uttryckligen godkänts.

3.2 Upprätthålla strikt separation mellan test- och produktionssystem för att undvika oavsiktlig dataexponering eller påverkan på driften.

3.3 Skydda testsystem och testdata mot obehörig åtkomst, oavsiktligt röjande eller återanvändning mellan miljöer utan lämpliga kontroller.

3.4 Uppfylla tillämpliga dataskyddskrav (t.ex. GDPR och NIS2) genom att säkerställa att all testdata behandlas lagligt, korrekt och säkert.

3.5 Stödja organisationens beredskap för externa revisioner och ISO/IEC 27001-certifiering genom att dokumentera testpraxis och tillämpa enhetliga skyddsåtgärder.

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Har det övergripande ansvaret för skydd av testdata och säkerheten i testsystem.

4.1.2 Godkänner all användning av verkliga data i testning efter att ha säkerställt att lämpliga skyddsåtgärder har införts (t.ex. anonymisering eller datamaskering).

4.1.3 Verifierar att testaktiviteter dokumenteras korrekt och följer denna policy.

4.2 Projektägare

4.2.1 Samordnar utformning och genomförande av testprocesser.

4.2.2 Säkerställer att alla teammedlemmar förstår och följer denna policy.

4.2.3 Bekräftar att testsystem är säkert konfigurerade innan testning påbörjas.

4.2.4 Rapporterar incidenter som rör testmiljöer eller dataläckage till GM.

[... 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 Planerade granskningar

9.1.1 Denna policy ska granskas minst en gång per år av verkställande direktör (GM). Granskningen ska säkerställa att policyn förblir aktuell i förhållande till:

9.1.1.1 Förändringar i verktyg, plattformar eller miljöer för programvaruutveckling

9.1.1.2 Uppdaterade rättsliga skyldigheter, inklusive krav avseende dataskydd eller digital operativ motståndskraft

9.1.1.3 Certifiering för små och medelstora företag och revisionsberedskap enligt ISO/IEC 27001

9.2 Utlösande händelser för mellanliggande granskning

9.2.1 Ytterligare granskningar ska genomföras efter:

9.2.1.1 Incidenter som omfattar dataexponering eller kompromettering i testmiljöer

9.2.1.2 Användning av verkliga data i testning, även om de är anonymiserade

9.2.1.3 Införande av nya testmetoder, system eller leverantörer

9.2.1.4 Regulatoriska uppdateringar som påverkar hur data hanteras under testning

9.3 Ändringshantering och kommunikation

9.3.1 GM ansvarar för att:

9.3.1.1 Uppdatera denna policy och dokumentera eventuella revideringar i versionshistoriken

9.3.1.2 Informera personal, utvecklare och relevanta tjänsteleverantörer om uppdateringar

9.3.1.3 Bekräfta att all personal som arbetar med testning förstår och tillämpar de senaste kraven

9.3.1.4 Upprätthålla en tillgänglig version av den senaste policyn för granskning och revisionsändamål

9.4 Revision och dokumentation

9.4.1 Uppgifter om alla policygranskningar, godkännanden av användning av verkliga data och motiveringar för undantag ska:

9.4.1.1 Bevaras säkert för revisionsändamål

9.4.1.2 Vara tillgängliga på begäran vid interna revisioner eller revisioner utförda av tredje part

9.4.1.3 Granskas årligen för att säkerställa överensstämmelse med testpraxis

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med följande SME-policyer för att upprätthålla säkerhet och efterlevnad under testning:

10.1.1 P2S – Policy för styrningsroller och ansvar: Definierar vem som ansvarar för styrning av utveckling, testning och ansvar för miljöseparering.

10.1.2 P4S – Åtkomstkontrollpolicy: Reglerar tilldelning, hantering och borttagning av autentiseringsuppgifter för åtkomst till testsystem.

10.1.3 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att personalen förstår risker med testdata, säker hantering och korrekt separation av miljöer.

10.1.4 P13S – Policy för dataklassificering och märkning: Stödjer tydlig klassificering av testdata och vägleder strategier för anonymisering eller datamaskering.

10.1.5 P17S – Policy för dataskydd och integritet: Säkerställer anpassning till skyldigheter enligt EU:s GDPR, inklusive skyddsåtgärder för behandling och lagring av personuppgifter, även i testmiljöer.

10.1.6 P24S – Policy för säker utveckling: Anger övergripande säkerhetskrav för utvecklingsteam, inklusive säker användning av data under testfaser.

10.1.7 P30S – Policy för incidenthantering: Anger hur organisationen ska agera vid överträdelser eller andra problem som upptäcks i en testmiljö eller orsakas av felaktig hantering av testdata.

10.2 Dessa policyer utgör ett sammanhållet säkerhetsramverk för att stödja testintegritet, uppgiftsminimering och full anpassning till ISO/IEC 27001 inom utvecklings- och testverksamhet.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Kräver riskbedömning och riskbehandlingsåtgärder, inklusive risker relaterade till testning.

11.1.2 Klausul 8.1 – Kräver planering och styrning av operativa processer, inklusive miljöer för etablering av testsystem.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.28 – Kräver att organisationer skyddar testdata och säkerställer att den inte innehåller känsliga data eller produktionsdata.

11.2.2 Kontroll 8.29 – Kräver tydlig separation mellan utvecklings-, test- och produktionsmiljöer.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Omfattar krav på kontroller för utveckling och testning.

11.3.2 SA-12 – Behandlar risker i leveranskedjan kopplade till testning och säkerhetsutvärderingar.

11.3.3 SC-32 – Kräver separation av miljöer och skydd av testdatas konfidentialitet och riktighet.

11.4 EU:s allmänna dataskyddsförordning (GDPR)

11.4.1 Artikel 5.1 c – Kräver uppgiftsminimering, inklusive att endast nödvändiga data används för testning.

11.4.2 Artikel 25 – Kräver inbyggt dataskydd, vilket omfattar kontroller för testmiljöer.

11.4.3 Artikel 32 – Kräver säker behandling av personuppgifter i alla system, inklusive icke-produktionsmiljöer.

11.5 EU:s NIS2-direktiv (2022/2555)

11.5.1 Artikel 21.2 e, h – Kräver säker utveckling och systemtestning, särskilt där digitala tjänster exponeras för cyberrisker.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9 – Betonar vikten av digital operativ motståndskraft, inklusive säker testning av IKT-system av små och medelstora företag i finanssektorn.

11.7 COBIT 2019

11.7.1 BAI07 – Hantera ändringsacceptans och övergång: Omfattar testkontroller för att validera nya system och datahantering.

11.7.2 DSS05 – Hantera säkerhetstjänster: Kräver test- och utvecklingspraxis som förhindrar missbruk eller exponering av verksamhetsinformation.