					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P29S					Titlul documentului: **Politica privind datele de testare și mediile de testare**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1, 8	
ISO/IEC 27002:2022	Controalele 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
GDPR	Articolele 5 alin. (1) lit. (c), 25, 32	
Directiva UE NIS2	Articolul 21 alin. (2) lit. (e), (h)	
Regulamentul UE DORA	Articolul 9	
COBIT 2019	BAI07, DSS05	

1. Scop

1.1 Prezenta politică stabilește modul în care trebuie gestionate datele de testare și mediile de testare pentru a preveni expunerea accidentală, incidentele de securitate a datelor sau perturbările operaționale în timpul activităților de testare.

1.2 Aceasta asigură că datele reale ale clienților nu sunt utilizate necorespunzător în timpul testării aplicațiilor software sau a sistemelor și că mediile de testare sunt separate logic și tehnic de sistemele de producție.

1.3 Politica este concepută pentru a sprijini IMM-urile în respectarea cerințelor de certificare ISO/IEC 27001 și a legislației relevante privind protecția datelor, menținând totodată un caracter practic și aplicabil pentru organizațiile fără o echipă IT dedicată.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor:

2.1.1 tuturor mediilor de testare (de exemplu, servere de preproducție, sisteme sandbox, platforme de testare pentru dezvoltare)

2.1.2 tuturor datelor de testare, indiferent dacă sunt create manual, generate sau derivate din date de producție

2.1.3 întregului personal implicat în activități de testare, inclusiv angajați, contractori, colaboratori independenți și furnizori de servicii IT

2.1.4 oricărei activități de testare care poate afecta platforme destinate clienților, sisteme interne ale organizației sau servicii ale terților

2.2 Aceasta acoperă atât mediile tehnice, cât și procesele utilizate pentru a sprijini:

2.2.1 dezvoltarea site-urilor web, a aplicațiilor și a instrumentelor

2.2.2 upgrade-urile de sistem, testarea configurațiilor și testarea integrării

2.2.3 testele funcționale sau de securitate, automate și manuale

3. Obiective

3.1 Prevenirea utilizării în testare a datelor reale și identificabile ale clienților, cu excepția cazului în care acestea sunt anonimizate și aprobate explicit.

3.2 Menținerea unei separări stricte între sistemele de testare și cele de producție, pentru a evita expunerea neintenționată a datelor sau interferențele operaționale.

3.3 Protejarea sistemelor și a datelor de testare împotriva accesului neautorizat, divulgării accidentale sau reutilizării între medii fără controale adecvate.

3.4 Respectarea reglementărilor aplicabile privind protecția datelor (de exemplu, GDPR, NIS2), prin asigurarea faptului că toate datele de testare sunt prelucrate în mod legal, echitabil și securizat.

3.5 Sprijinirea capacității organizației de a demonstra conformitatea în cadrul auditurilor externe și pentru certificarea ISO/IEC 27001, prin documentarea practicilor de testare și aplicarea consecventă a măsurilor de protecție.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Are responsabilitatea generală pentru protecția datelor de testare și securitatea sistemelor de testare.

4.1.2 Aprobă orice utilizare a datelor reale în testare, după confirmarea existenței unor măsuri de protecție adecvate (de exemplu, anonimizare sau mascarea datelor).

4.1.3 Verifică faptul că activitățile de testare sunt documentate corespunzător și respectă această politică.

4.2 Responsabil de proiect

4.2.1 Coordonează proiectarea și executarea proceselor de testare.

4.2.2 Se asigură că toți membrii echipei înțeleg și respectă această politică.

4.2.3 Confirmă că sistemele de testare sunt configurate în condiții de securitate înainte de începerea testării.

4.2.4 Raportează Directorului general orice incidente care implică mediile de testare sau scurgeri de date.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1 Revizuiri programate

9.1.1 Această politică trebuie revizuită cel puțin o dată pe an de către Directorul general. Revizuirea asigură că politica rămâne actualizată în raport cu:

9.1.1.1 modificările survenite în instrumentele, platformele sau mediile de dezvoltare software

9.1.1.2 obligațiile legale actualizate, inclusiv cerințele privind protecția datelor sau reziliența digitală

9.1.1.3 cerințele de certificare pentru IMM-uri și pregătirea pentru audit în temeiul ISO/IEC 27001

9.2 Evenimente declanșatoare pentru revizuirea intermediară

9.2.1 Revizuiri suplimentare trebuie efectuate după:

9.2.1.1 orice incident care implică expunerea datelor sau compromiterea mediilor de testare

9.2.1.2 utilizarea datelor reale în testare, chiar dacă acestea sunt anonimizate

9.2.1.3 introducerea unor noi metode de testare, sisteme sau furnizori

9.2.1.4 actualizări de reglementare care afectează modul de gestionare a datelor în timpul testării

9.3 Managementul schimbărilor și comunicare

9.3.1 Directorul general este responsabil pentru:

9.3.1.1 actualizarea acestei politici și documentarea oricăror revizuiri, inclusiv istoricul versiunilor

9.3.1.2 notificarea personalului, a dezvoltatorilor și a furnizorilor de servicii relevanți cu privire la actualizări

9.3.1.3 confirmarea faptului că tot personalul implicat în activități de testare înțelege și aplică cele mai recente reguli

9.3.1.4 menținerea unei versiuni accesibile a celei mai recente politici în scopuri de revizuire și audit

9.4 Audit și documentație

9.4.1 Înregistrările tuturor revizuirilor politicii, aprobărilor pentru utilizarea datelor reale și justificărilor pentru excepții trebuie:

9.4.1.1 să fie păstrate în condiții de securitate în scopuri de audit

9.4.1.2 să fie disponibile la cerere în cadrul auditurilor interne sau ale terților

9.4.1.3 să fie revizuite anual pentru a asigura consecvența cu practicile de testare

10. Politici corelate și interdependențe

10.1 Această politică trebuie aplicată în coordonare cu următoarele politici SME, pentru a menține securitatea și conformitatea în timpul testării:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: definește cine este responsabil pentru supravegherea dezvoltării, testării și responsabilităților privind separarea sistemelor.

10.1.2 P4S – Politica de control al accesului: reglementează atribuirea, gestionarea și eliminarea datelor de autentificare pentru accesul la sistemele de testare.

10.1.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: asigură că personalul înțelege riscurile aferente datelor de testare, practicile de gestionare securizată și separarea corespunzătoare a mediilor.

10.1.4 P13S – Politica de clasificare și etichetare a datelor: sprijină clasificarea clară a datelor de testare și orientează strategiile de anonimizare sau de mascarea datelor.

10.1.5 P17S – Politica de protecție a datelor și confidențialitate: se aliniază obligațiilor GDPR, inclusiv măsurilor de protecție privind prelucrarea și stocarea datelor cu caracter personal, inclusiv în mediile de testare.

10.1.6 P24S – Politica de dezvoltare securizată: stabilește cerințele generale de securitate pentru echipele de dezvoltare, inclusiv utilizarea în siguranță a datelor în etapele de testare.

10.1.7 P30S – Politica de răspuns la incidente: descrie modul de răspuns la orice încălcare sau problemă identificată într-un mediu de testare sau cauzată de gestionarea necorespunzătoare a datelor de testare.

10.2 Aceste politici formează un cadru unificat de securitate pentru a sprijini integritatea testării, reducerea la minimum a datelor și alinierea deplină la ISO/IEC 27001 în toate operațiunile de dezvoltare și asigurare a calității.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1 – impune evaluarea riscurilor și acțiuni de tratare a riscurilor, inclusiv pentru riscurile asociate testării.

11.1.2 Clauza 8.1 – impune planificarea și controlul proceselor operaționale, inclusiv al mediilor utilizate pentru configurarea sistemelor de testare.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.28 – impune organizațiilor să protejeze datele de testare și să se asigure că acestea nu conțin date sensibile sau date de producție.

11.2.2 Controlul 8.29 – impune separarea clară a mediilor de dezvoltare, testare și producție.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – acoperă cerințele de control privind dezvoltarea și testarea.

11.3.2 SA-12 – abordează riscurile de testare din lanțul de aprovizionare și evaluările de securitate.

11.3.3 SC-32 – impune separarea mediilor și protecția confidențialității și integrității datelor de testare.

11.4 Regulamentul general privind protecția datelor (GDPR)

11.4.1 Articolul 5 alin. (1) lit. (c) – impune reducerea la minimum a datelor, inclusiv utilizarea exclusivă a datelor necesare pentru testare.

11.4.2 Articolul 25 – impune protecția datelor începând cu momentul proiectării, inclusiv prin controale aplicabile mediilor de testare.

11.4.3 Articolul 32 – impune prelucrarea securizată a datelor cu caracter personal în toate sistemele, inclusiv în mediile care nu sunt de producție.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolul 21 alin. (2) lit. (e), (h) – impune dezvoltarea securizată și testarea sistemelor, în special acolo unde serviciile digitale sunt expuse la risc cibernetic.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 9 – subliniază importanța rezilienței operaționale digitale, inclusiv a testării securizate a sistemelor TIC de către IMM-urile din sectorul financiar.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: include controale de testare pentru validarea noilor sisteme și a gestionării datelor.

11.7.2 DSS05 – Manage Security Services: impune practici de testare și dezvoltare care previn utilizarea necorespunzătoare sau expunerea datelor organizației.