					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P29					Titlul documentului: **Politica privind datele de test 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	Clauza 8	Relevantă pentru planificarea și controlul securizat al datelor de test și al mediilor de testare
ISO/IEC 27002:2022	Controalele 8.28–8.29	Acoperă securizarea datelor de test și protecția mediilor de testare
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Abordează testarea și evaluarea realizate de dezvoltatori, protecția datelor în repaus și integritatea informațiilor
GDPR al UE	Articolele 5, 25, 32	Acoperă reducerea la minimum a datelor, protecția datelor începând cu faza de proiectare și securitatea prelucrării în contexte de testare
Directiva NIS2 a UE	Articolul 21(2)(e), (h)	Se referă la practici securizate de dezvoltare și testare
Regulamentul DORA al UE	Articolul 9	Vizează sistemele și protocoalele TIC, precum și securitatea datelor de test
COBIT 2019	DSS05, BAI07	Abordează managementul serviciilor de securitate și acceptarea/tranziția schimbărilor

1. Scop

1.1. Prezenta politică definește cerințele obligatorii pentru gestionarea mediilor de testare și a datelor de test, pentru a asigura securitatea, confidențialitatea și integritatea operațională pe întreg ciclul de viață al dezvoltării și testării software.

1.2. Politica are ca scop prevenirea accesului neautorizat, a scurgerilor de date și a contaminării sistemelor de producție prin utilizarea necorespunzătoare a mediilor de testare sau prin folosirea datelor reale în activitățile de testare.

1.3. Politica impune gestionarea securizată a datelor utilizate pentru testare, hardenizarea infrastructurii de testare și controale de acces bazate pe roluri, în concordanță cu obligațiile de reglementare și contractuale aplicabile.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor mediilor de testare, datelor, instrumentelor și proceselor utilizate pentru testarea software-ului, sistemelor, aplicațiilor și infrastructurii din cadrul organizației.

2.2. Politica acoperă:

2.2.1. Mediile de testare alocate on-premises, în cloud sau prin intermediul platformelor terțe

2.2.2. Datele de test utilizate în testarea funcțională, de performanță, de regresie și de securitate

2.2.3. Testarea manuală, bazată pe scripturi sau automatizată (de exemplu, fluxuri de integrare și livrare continuă (CI/CD))

2.2.4. Întregul personal implicat în activitățile de testare, inclusiv echipe interne, furnizori și contractori

2.3. Politica se aplică indiferent de criticitatea sistemului, tipul aplicației sau dacă dezvoltarea este internă ori externalizată.

3. Obiective

3.1. Prevenirea utilizării în mediile de testare a datelor active, sensibile sau reglementate (de exemplu, informații de identificare personală (PII), date ale deținătorilor de carduri), cu excepția cazului în care acestea sunt anonimizate sau aprobate în mod specific.

3.2. Asigurarea unei separări complete, la nivel de rețea și de acces, între mediile de testare și cele de producție, pentru a evita accesul neautorizat la date sau contaminarea sistemelor.

3.3. Impunerea criptării, a mascării datelor sau a generării de date sintetice atunci când sunt necesare date reprezentative în scopuri de testare.

3.4. Reducerea probabilității apariției unor neconformități, a expunerii datelor clienților sau a perturbării activităților operaționale ale organizației ca urmare a utilizării unor date de test sau a unor medii de testare nesecurizate.

3.5. Alinierea gestionării datelor de test la standardele din industrie (ISO, NIST, COBIT) și la reglementări precum GDPR, NIS2 și DORA.

4. Roluri și responsabilități

4.1. Directorul de securitate a informațiilor (CISO)

4.1.1. Deține responsabilitatea pentru această politică și impune măsuri tehnice și administrative de protecție pentru datele de test și mediile de testare.

4.1.2. Aprobă utilizarea datelor reale sau sensibile în testare, pe baza unei justificări adecvate și a unor controale compensatorii.

4.2. Responsabilii QA/Test

4.2.1. Coordonează planificarea testării și se asigură că toate activitățile de testare respectă cerințele prezentei politici.

4.2.2. Validează separarea adecvată a mediilor, accesul și pregătirea datelor pentru fiecare etapă de testare.

[... 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. Prezenta politică trebuie revizuită anual și actualizată, după caz, pentru a reflecta:

9.1.1. Modificările cerințelor de reglementare (de exemplu, GDPR, DORA, NIS2)

9.1.2. Adoptarea unor noi instrumente, platforme sau fluxuri de automatizare pentru testare

9.1.3. Constatările auditului intern sau recomandările rezultate în urma incidentelor

9.1.4. Extinderea proceselor de dezvoltare sau QA care modifică gestionarea datelor de test ori utilizarea mediilor de testare

9.2. CISO răspunde de inițierea revizuirii în colaborare cu:

9.2.1. Responsabilii QA/Test

9.2.2. Managerii DevOps și de infrastructură

9.2.3. Echipele de dezvoltare a aplicațiilor

9.2.4. Responsabilul cu protecția datelor și consilierul juridic

9.3. Toate reviziile trebuie:

9.3.1. Să fie supuse controlului versiunilor și stocate în depozitul central de documente

9.3.2. Să fie comunicate personalului vizat prin canale formale (de exemplu, notificări SMSI, sesiuni de informare ale echipei)

9.3.3. Să fie corelate cu actualizările standardelor tehnice, controalelor și procedurilor operaționale asociate

9.4. Revizuirile intermediare declanșate de evenimente trebuie efectuate imediat după orice:

9.4.1. Scurgere de date sau incident de securitate care implică medii de testare

9.4.2. Neconformitate de audit legată de gestionarea datelor de test

9.4.3. Modificare semnificativă a obligațiilor legale sau a arhitecturii IT

10. Politici conexe și interdependențe

10.1. Prezenta politică este strâns integrată cu următoarele politici, pentru a asigura gestionarea securizată și conformă a datelor de test și a mediilor de testare:

10.1.1. P1 – Politica de securitate a informațiilor: stabilește principiile generale de securitate care guvernează protecția datelor de test și gestionarea mediilor de testare.

10.1.2. P5 – Politica de management al schimbărilor: se aplică creării, actualizării și dezafectării mediilor de testare, precum și fluxurilor de implementare.

10.1.3. P13 – Politica de clasificare și etichetare a datelor: ghidează selectarea datelor de test și aplicarea controalelor în funcție de sensibilitate.

10.1.4. P14 – Politica de păstrare și eliminare a datelor: definește termenele de păstrare și cerințele de eliminare securizată pentru seturile de date de test.

10.1.5. P15 – Politica de backup și restaurare: impune practicile de backup și validarea recuperării pentru mediile de testare.

10.1.6. P18 – Politica privind controalele criptografice: stabilește standardele obligatorii de criptare pentru datele în repaus și în tranzit în cadrul platformelor de testare.

10.1.7. P22 – Politica de jurnalizare și monitorizare: reglementează vizibilitatea și detectarea anomaliilor pentru activitățile din mediile de testare.

10.1.8. P30 – Politica de răspuns la incidente: definește escaladarea și remedierea pentru încălcări sau incidente care implică sisteme de test.

10.1.9. P33 – Politica de audit și monitorizare a conformității: permite validarea respectării politicii și asigurarea continuă.

11. Standarde și cadre de referință

11.1. Prezenta politică este aliniată la standarde globale de securitate cibernetică și cadre de reglementare care impun gestionarea securizată a datelor de test și protecția mediilor non-producție.

11.2. ISO/IEC 27001:

11.2.1. Clauza 8.1 - impune planificarea și controlul securizat al datelor de test și al mediilor de testare.

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

11.3.1. Anexa A, controlul 8.28 – Date de test securizate: impune protejarea datelor de test utilizate în etapele de dezvoltare și testare prin anonimizare, mascarea datelor sau generare de date sintetice.

11.3.2. Anexa A, controlul 8.29 – Protecția mediilor de testare: impune separarea față de producție, controale de acces și hardenizarea mediilor pentru sistemele de test.

11.3.3. Aceste controale stabilesc cerințe pentru gestionarea securizată a datelor utilizate în timpul testării și pentru protejarea sistemelor non-producție împotriva utilizării necorespunzătoare, compromiterii sau contaminării.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testare și evaluare realizate de dezvoltatori: stabilește așteptările privind proceduri de testare securizate și repetabile, cu controale adecvate asupra datelor.

11.4.2. SC-28 – Protecția informațiilor în repaus: este aliniat cu criptarea datelor de test stocate în sisteme non-producție.

11.4.3. SC-32 – Integritatea informațiilor: susține validarea datelor, prevenirea coruperii și controalele de intrare/ieșire în timpul testării.

11.5. GDPR al UE (2016/679):

11.5.1. Articolul 5 – Reducerea la minimum a datelor: interzice utilizarea inutilă a datelor cu caracter personal în testare.

11.5.2. Articolul 25 – Protecția datelor începând cu faza de proiectare: impune aplicarea tehnicilor de protecție a datelor încă de la începutul ciclului de dezvoltare și testare.

11.5.3. Articolul 32 – Securitatea prelucrării: impune măsuri de protecție pentru mediile de testare care prelucrează date cu caracter personal sau date sensibile.

11.6. Directiva NIS2 a UE (2022/2555):

11.6.1. Articolul 21(2)(e, h): impune procese securizate de dezvoltare și testare software, cu accent pe protecția împotriva accesului neautorizat și a scurgerilor de date.

11.7. Regulamentul DORA al UE (2022/2554):

11.7.1. Articolul 9 – Sisteme și protocoale TIC: impune ca procesele de testare să susțină reziliența și să protejeze datele operaționale împotriva compromiterii sau divulgării neautorizate.

11.8. COBIT 2019:

11.8.1. DSS05 – Managementul serviciilor de securitate: susține aplicarea politicilor de securitate în toate mediile, inclusiv în cele non-producție.

11.8.2. BAI07 – Managementul acceptării schimbărilor și al tranziției: acoperă procesul formal de tranziție din testare în producție, inclusiv controalele asupra datelor și mediilor.