					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P16					Titlul documentului: **Politica de mascare a datelor și pseudonimizare**							
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 6.1	Cerințe generale privind managementul riscurilor și controalele operaționale pentru mascarea datelor și pseudonimizare
ISO/IEC 27002:2022	Controalele 8.11, 8	Ghid pentru implementarea mascării datelor și a pseudonimizării
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Controale privind confidențialitatea și protecția datelor pentru reducerea la minimum a datelor, transformarea acestora și limitarea accesului
GDPR al UE	Articolele 4(5), 5(1)(c,f), 32	Temeiul juridic și cerințele privind pseudonimizarea și măsurile de protecție a datelor
Directiva NIS2 a UE	Articolul 21(2)(c)	Obligația de a implementa măsuri tehnice și organizatorice, inclusiv tehnologii de îmbunătățire a confidențialității (PET)
Regulamentul DORA al UE	Articolele 10(1), 10(2)(e)	Managementul riscurilor TIC și controale de confidențialitate pentru mascarea datelor și pseudonimizare
COBIT 2019	DSS05.01, DSS06.06, MEA	Controale de guvernanță pentru protecția datelor prin utilizarea mascării datelor și evaluarea conformității

1. Scop

1.1 Această politică definește abordarea organizației privind implementarea mascării datelor și a pseudonimizării ca tehnologii de îmbunătățire a confidențialității (PET), în vederea reducerii posibilității de identificare și a expunerii datelor cu caracter personal sau a datelor sensibile.

1.2 Aceasta susține utilizarea securizată a informațiilor în activitățile de testare, analiză și operare ale organizației, asigurând totodată conformitatea cu cerințele legale și de reglementare, atenuarea impactului unui incident de securitate și aplicarea principiilor reducerii la minimum a datelor și confidențialității.

1.3 Politica este aliniată la ISO/IEC 27001:2022, susține articolul 4 alineatul (5) din GDPR privind pseudonimizarea și integrează o implementare bazată pe risc, în concordanță cu standardele NIST, NIS2, DORA și COBIT 2019.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor categorii:

2.1.1 întregului personal, contractorilor, terților și furnizorilor care au acces la sisteme ce gestionează informații cu caracter personal, confidențiale sau sensibile.

2.1.2 tuturor mediilor de date, inclusiv mediilor de producție, dezvoltare, testare și preproducție.

2.1.3 tuturor formelor de mascarea datelor (de exemplu, statică, dinamică, deterministă, tokenizare) și tehnicilor de pseudonimizare utilizate pentru reducerea riscurilor privind confidențialitatea.

2.1.4 tuturor tipurilor de date (structurate sau nestructurate), sistemelor (on-premises sau din cloud) și aplicațiilor care implică date cu caracter personal sau date reglementate.

2.2 Domeniul de aplicare include utilizarea în:

2.2.1 dezvoltarea aplicațiilor și medii de asigurare a calității/testare

2.2.2 platforme de analiză sau raportare

2.2.3 schimbul de date cu terți sau furnizori de servicii

2.2.4 sisteme de backup, arhivare sau recuperare

3. Obiective

3.1 Asigurarea unei aplicări consecvente și eficace a mascării datelor și a pseudonimizării pentru reducerea riscurilor de expunere sau utilizare abuzivă a datelor.

3.2 Asigurarea faptului că datele reale nu sunt utilizate niciodată în medii non-producție, cu excepția cazului în care au fost transformate prin tehnici PET aprobate.

3.3 Menținerea integrității referențiale, a utilizabilității și a transformărilor cu păstrarea formatului, atunci când acest lucru este necesar pentru consecvența operațională.

3.4 Aplicarea unor controale stricte de acces la datele originale, datele mascate și cheile de reidentificare.

3.5 Tratarea seturilor de date mascate sau pseudonimizate ca date sensibile, supuse jurnalizării accesului, controalelor de retenție și protocoalelor de răspuns la incidente.

3.6 Validarea eficacității acestor controale prin testare continuă, monitorizare și proceduri de audit.

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 aprobă această politică și asigură aplicarea acesteia ca parte a inițiativelor mai ample de guvernanță IT și protecție a datelor.

4.2 Directorul de securitate a informațiilor (CISO) / Managerul SMSI

4.2.1 asigură supravegherea implementării și a conformității continue.

4.2.2 asigură alinierea la ISO/IEC 27001, clauza 6.1.3 (tratamentul riscurilor) și clauza 8.1 (control operațional).

4.2.3 revizuiește jurnalele de audit și validează eficacitatea controalelor.

[... 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 Această politică trebuie revizuită cel puțin anual sau mai devreme în cazul:

9.1.1 modificărilor de reglementare care afectează mascarea datelor sau pseudonimizarea

9.1.2 adoptării unor noi sisteme IT care gestionează date sensibile

9.1.3 modificărilor semnificative ale schemei de clasificare a datelor a organizației

9.1.4 constatărilor de audit care indică deficiențe ale controalelor

9.1.5 apariției unor noi amenințări sau tehnologii de mascarea datelor

9.2 Managerul SMSI trebuie să conducă revizuirea în consultare cu DPO-ul, proprietarii datelor, echipa de securitate IT și departamentul juridic. Actualizările trebuie să facă obiectul controlului versiunilor, să fie aprobate de conducerea executivă și comunicate tuturor părților interesate afectate.

10. Politici conexe și interdependențe

10.1 P13 - Politica de clasificare și etichetare a datelor. Deciziile privind mascarea datelor și pseudonimizarea depind direct de clasificarea câmpurilor de date și de nivelurile de sensibilitate definite în P13.

10.2 P14 - Politica de păstrare și eliminare a datelor. Seturile de date transformate trebuie păstrate și eliminate în conformitate cu regulile privind ciclul de viață prevăzute în P14, asigurând tratarea datelor mascate și pseudonimizate ca date sensibile.

10.3 P17 - Politica de protecție a datelor și confidențialitate. Oferă principiile de confidențialitate și fundamentul de reglementare pentru aplicarea pseudonimizării ca activitate de prelucrare conformă cu GDPR și cu acte normative similare.

10.4 P22 - Politica de jurnalizare și monitorizare. Permite auditarea și alertarea centralizată a evenimentelor de mascarea datelor și pseudonimizare, în conformitate cu protocoale structurate de monitorizare a securității.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1.3 - Plan de tratare a riscurilor: stabilește mascarea datelor și pseudonimizarea ca mecanisme de tratare a riscurilor pentru reducerea posibilității de identificare a datelor sensibile în medii de prelucrare neesențiale.

11.1.2 Clauza 8.1 - Planificare și control operațional: impune controale tehnice și procedurale pentru transformarea securizată a datelor în timpul prelucrării, stocării sau transferului.

11.2 ISO/IEC 27002:2022

11.2.1 Controalele 8.11, 8: orientări privind mascarea datelor și pseudonimizarea pentru reducerea la minimum a riscurilor de reidentificare și a scurgerilor de date.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protecția PII: implementarea tehnologiilor de îmbunătățire a confidențialității, cum ar fi mascarea datelor și pseudonimizarea.

11.3.2 PT-2, PT-3: reducerea la minimum a PII și securitatea prelucrării - transformare pentru reducerea posibilității de identificare și aplicarea controalelor de acces.

11.3.3 SC-12, SC-28, SC-30: confidențialitatea și integritatea datelor - controale de confidențialitate și obscurizare pentru stocare, transmitere și utilizare.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 4(5): definiția formală a pseudonimizării.

11.4.2 Articolul 32: securitatea prelucrării - măsuri organizatorice și tehnice pentru pseudonimizare.

11.4.3 Articolul 5(1)(c,f): reducerea la minimum a datelor și confidențialitate prin utilizarea pseudonimizării și mascării datelor.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(c): impune utilizarea PET, cum ar fi mascarea datelor și pseudonimizarea, ca măsuri de securitate.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 10(1): cadrul de management al riscurilor TIC include controale privind mascarea datelor și pseudonimizarea.

11.6.2 Articolul 10(2)(e): impune utilizarea tehnologiilor de transformare pentru protejarea datelor cu caracter personal și a datelor financiare.

11.7 COBIT 2019

11.7.1 DSS05.01: Protejarea activelor informaționale - cerințe pentru mascarea datelor și pseudonimizare.

11.7.2 DSS06.06: Testare și analiză securizate - mascarea datelor în medii din afara producției.

11.7.3 MEA03: monitorizarea conformității pentru eficacitatea mascării datelor și pseudonimizării.