					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P24					Titlul documentului: **Politica de dezvoltare securizată**							
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**

1. Scop

1.1 Această politică stabilește cerințele obligatorii de securitate pentru activitățile de dezvoltare software și de sisteme din cadrul organizației, inclusiv proiectele interne, dezvoltarea externalizată și integrarea codului provenit de la terți.

1.2 Obiectivul este asigurarea integrării securității pe întreg ciclul de viață al dezvoltării software (SDLC), precum și identificarea, reducerea și prevenirea vulnerabilităților înainte de implementarea în producție.

1.3 Această politică sprijină aplicarea ISO/IEC 27001:2022, clauza 8.1, precum și a controalelor din Anexa A 8.25–8, prin standardizarea guvernanței dezvoltării securizate, a practicilor de validare a codului și a supravegherii dezvoltării realizate de terți.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor elementelor de mai jos:

2.1.1 software-ului, aplicațiilor, scripturilor, integrărilor și instrumentelor de automatizare dezvoltate intern sau extern

2.1.2 echipelor de dezvoltare, proprietarilor de produs, echipelor DevOps, echipelor de asigurare a calității (QA), arhitecților, managerilor de proiect și contractorilor

2.1.3 mediilor SDLC, inclusiv sistemelor de dezvoltare, testare, staging și preproducție

2.1.4 componentelor open-source și componentelor provenite de la terți integrate în aplicațiile interne

2.1.5 software-ului implementat on-premises, în medii cloud private, hibride sau publice

2.2 Toți utilizatorii și toate entitățile care participă la dezvoltarea, testarea sau implementarea sistemelor în contextul organizațional intră sub incidența acestei politici, inclusiv furnizorii de servicii administrate (MSP) și furnizorii de platforme.

3. Obiective

3.1 Integrarea controalelor de securitate în toate etapele dezvoltării software, de la proiectare până la implementare, astfel încât reducerea riscurilor să fie proactivă și continuă.

3.2 Prevenirea introducerii unor vulnerabilități exploatabile, precum defecte de tip injection, mecanisme de autentificare nesecurizate și expunerea la puncte slabe cunoscute ale componentelor provenite de la terți.

3.3 Stabilirea și aplicarea practicilor de programare securizată aliniate la OWASP, SANS CWE și ghidurilor specifice cadrului tehnologic utilizat.

3.4 Asigurarea faptului că întregul cod este supus revizuirii de către colegi, analizei automatizate și validării de securitate înainte de implementare.

3.5 Gestionarea riscurilor de dezvoltare generate de activități externalizate, de includerea codului provenit de la terți și de reutilizarea software-ului open-source.

3.6 Protejarea mediilor de dezvoltare, testare și staging împotriva accesului neautorizat și prevenirea utilizării datelor de producție fără mascarea sau anonimizarea aprobate ale datelor.

3.7 Promovarea conștientizării securității în rândul dezvoltatorilor, managerilor de produs și specialiștilor în asigurarea calității, prin instruire specifică rolului și actualizări continue privind riscurile emergente.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Este responsabil de această politică și se asigură că cerințele privind dezvoltarea securizată sunt aplicate la nivelul întregii organizații.

4.1.2 Aprobă standardele de programare securizată și acordurile privind dezvoltarea realizată de terți.

4.1.3 Validează deciziile de tratare a riscului pentru vulnerabilitățile nerezolvate sau amânate.

4.2 Responsabilul pentru securitatea aplicațiilor / Managerul DevSecOps

4.2.1 Elaborează, menține și promovează ghidurile privind programarea securizată.

4.2.2 Integrează testarea statică și dinamică de securitate în fluxurile de integrare și livrare continuă (CI/CD).

4.2.3 Efectuează revizuiri de securitate ale codului și stabilește acțiunile obligatorii de remediere.

[... 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 anual sau mai frecvent, ca răspuns la:

9.1.1 modificări majore ale metodologiilor de dezvoltare sau ale instrumentelor DevOps

9.1.2 incidente de securitate semnificative generate de vulnerabilități ale aplicațiilor

9.1.3 modificări ale cerințelor de reglementare privind software-ul securizat (de exemplu, GDPR, DORA)

9.1.4 standarde noi din industrie sau informații privind amenințările (de exemplu, OWASP Top 10, SLSA, MITRE CWE)

9.2 Revizuirea politicii trebuie coordonată de Responsabilul pentru securitatea aplicațiilor, în colaborare cu CISO, arhitecții software, conducerea QA și consilierul juridic (pentru implicațiile legate de codul provenit de la terți).

9.3 Orice revizuire trebuie înregistrată în Registrul documentelor al SMSI, să fie supusă controlului versiunilor și comunicată echipelor afectate prin note de lansare sau instruire obligatorie.

9.4 Versiunile anterioare trebuie păstrate în depozitul de arhivă pentru asigurarea trasabilității juridice și de audit.

10. Politici asociate și interdependențe

10.1 P1 – Politica de securitate a informației. Stabilește mandatul strategic pentru integrarea securității în toate sistemele informatice ale organizației, iar dezvoltarea securizată reprezintă un control operațional fundamental.

10.2 P4 – Politica de control al accesului. Definește măsurile de control pentru restricționarea accesului la mediile de dezvoltare, depozite, instrumente de build și fluxuri de integrare și livrare continuă (CI/CD).

10.3 P5 – Politica de management al schimbărilor. Asigură că modificările de cod, lansările și implementările fac obiectul aprobării corespunzătoare, al planificării revenirii și al verificării post-implementare.

10.4 P12 – Politica de management al activelor. Sprijină inventarierea mediilor de dezvoltare, a depozitelor sursă și a sistemelor de build ca active gestionate, supuse clasificării și protecției.

10.5 P22 – Politica de jurnalizare și monitorizare. Se aplică fluxurilor de dezvoltare, asigurând că procesele de build, promovările de cod și evenimentele de implementare sunt jurnalizate, monitorizate și analizate pentru identificarea anomaliilor de securitate.

10.6 P30 – Politica de răspuns la incidente. Oferă cadrul pentru analizarea și tratarea defectelor de securitate identificate după implementare sau în timpul testării de securitate a aplicațiilor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Planificare și control operațional: impune integrarea proceselor și controalelor de dezvoltare securizată în activitățile operaționale ale organizației.

11.2 ISO/IEC 27002:2022 – Controalele 8.25–8

11.2.1 Controlul 8.25 din Anexa A – Ciclul de viață al dezvoltării securizate: impune includerea formală a securității în proiectarea și dezvoltarea software-ului.

11.2.2 Controlul 8.26 din Anexa A – Cerințe de securitate ale aplicațiilor: impune definirea programării securizate și a criteriilor de acceptare din perspectiva securității.

11.2.3 Controlul 8.27 din Anexa A – Principii de arhitectură și inginerie a sistemelor securizate: impune aplicarea principiilor de proiectare a securității și reducerea punctelor slabe cunoscute.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 până la SA-15: stabilesc practici structurate de dezvoltare securizată a aplicațiilor, inclusiv cerințe privind proiectarea, integritatea codului și testarea.

11.3.2 SI-10 – Validarea datelor de intrare: abordează măsuri de apărare prin programare securizată.

11.3.3 SR-3 – Protecția lanțului de aprovizionare: impune evaluarea software-ului provenit de la terți, a componentelor și a furnizorilor de dezvoltare.

11.4 GDPR (UE) 2016/679

11.4.1 Articolul 25 – Protecția datelor începând cu momentul conceperii și în mod implicit: impune integrarea securității și a confidențialității în dezvoltarea sistemelor.

11.4.2 Articolul 32 – Securitatea prelucrării: susține măsuri tehnice precum validarea datelor de intrare, controalele de acces și implementarea securizată.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolul 21(2)(e–f): impune practici de dezvoltare software care includ managementul vulnerabilităților, securitatea codului și raportarea incidentelor.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: impune practici de dezvoltare securizată pentru entitățile financiare, inclusiv controale privind calitatea software-ului și remedierea defectelor.

11.6.2 Articolul 10 – Continuitatea activității și testare: încurajează testarea și validarea riguroasă a sistemelor TIC, inclusiv a aplicațiilor.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionarea identificării soluțiilor și dezvoltării: guvernează proiectarea, dezvoltarea și integrarea securității în soluțiile noi.

11.7.2 BAI07 – Gestionarea acceptării schimbării și a tranziției: asigură implementarea securizată și evaluarea post-implementare.

11.7.3 DSS05 – Gestionarea serviciilor de securitate: aplică validarea securității pentru software și furnizarea serviciilor.