					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P24S					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**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	Controale de securitate relevante pentru practicile operaționale, inclusiv dezvoltarea securizată
ISO/IEC 27002:2022	Controalele 8.25–8.27	Acoperă ciclul de viață al dezvoltării securizate, testarea și responsabilitățile de securitate ale dezvoltatorilor terți
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Abordează SDLC securizat, controlul accesului și managementul vulnerabilităților în dezvoltare
RGPD al UE	Articolul 25	Impune protecția datelor încă din faza de proiectare și în mod implicit în dezvoltarea software
Directiva NIS2 a UE	Articolul 21(2)(a), (e), (h)	Impune politici de dezvoltare securizată, supravegherea utilizării componentelor open-source și documentarea măsurilor de atenuare
Regulamentul DORA al UE	Articolele 6(7), 9(1)(c), 10(2)(c)	Securitatea ciclului de viață pentru sistemele TIC critice din sectorul financiar
COBIT 2019	BAI	Cadru pentru managementul dezvoltării securizate în mod structurat, cu trasabilitate și reziliență

1. Scop

1.1 Această politică asigură că toate aplicațiile software, scripturile și instrumentele web create sau modificate de organizație ori de partenerii săi externi sunt dezvoltate în condiții de securitate, reducând la minimum riscul de vulnerabilități, acces neautorizat la date sau perturbări operaționale.

1.2 Aceasta stabilește reguli obligatorii de dezvoltare securizată și practici de programare securizată care trebuie respectate de toți dezvoltatorii interni, contractanții și furnizorii, indiferent de dimensiunea sau complexitatea proiectului.

1.3 Această politică are rolul de a proteja datele clienților, de a preveni incidentele de securitate și de a asigura că software-ul creat sau personalizat de organizație ori pentru organizație poate trece audituri de securitate, poate îndeplini cerințele legale (de exemplu, RGPD, NIS2, DORA) și poate sprijini certificarea ISO/IEC 27001.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor persoanelor și entităților implicate, în numele organizației, în dezvoltarea, personalizarea, implementarea sau administrarea următoarelor:

2.1.1 Site-uri web, aplicații sau instrumente de automatizare

2.1.2 Scripturi sau aplicații software dezvoltate intern

2.1.3 Cod creat de dezvoltatori terți sau colaboratori independenți

2.1.4 Pluginuri, biblioteci și componente software integrate în sistemele de producție

2.2 Aceasta acoperă toate mediile utilizate în activitățile de dezvoltare, inclusiv:

2.2.1 Medii de dezvoltare și testare

2.2.2 Medii de staging și preproducție

2.2.3 Sisteme de producție utilizate pentru rularea codului dezvoltat la comandă

2.3 Politica reglementează, de asemenea, gestionarea datelor pe durata dezvoltării și implementării, în special orice utilizare a datelor de producție în sisteme non-producție.

3. Obiective

3.1 Prevenirea introducerii de defecte de securitate sau vulnerabilități în software-ul dezvoltat la comandă sau furnizat de terți.

3.2 Asigurarea integrării practicilor de programare securizată și a prevenirii vulnerabilităților în fiecare etapă a ciclului de viață al dezvoltării software.

3.3 Reducerea riscurilor asociate utilizării componentelor open-source sau ale terților prin impunerea unei evaluări corespunzătoare și a urmăririi acestora.

3.4 Impunerea revizuirii codului și a testării de securitate a aplicațiilor înainte de lansare.

3.5 Controlul accesului la mediile de dezvoltare și asigurarea separării acestora de sistemele de producție active.

3.6 Îndeplinirea cerințelor obligatorii prevăzute de standardele și reglementările internaționale (de exemplu, ISO/IEC 27001, RGPD, DORA, NIS2).

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Aprobă această politică și răspunde pentru aceasta.

4.1.2 Se asigură că toate activitățile de dezvoltare software, interne sau externalizate, respectă această politică.

4.1.3 Revizuiește și semnează contractele de dezvoltare sau de servicii care includ clauze privind dezvoltarea securizată.

4.1.4 Verifică respectarea cerințelor de către furnizori prin verificări periodice sau prin solicitarea de dovezi privind securitatea.

4.2 Dezvoltator intern sau proprietar de aplicație

4.2.1 Respectă practicile de programare securizată și procedurile de implementare.

4.2.2 Aplică lista de verificare pentru dezvoltare securizată fiecărui proiect.

4.2.3 Validează securitatea oricăror componente open-source sau ale terților utilizate.

4.2.4 Raportează imediat Directorului general orice vulnerabilitate identificată.

[... 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 de Directorul general cel puțin o dată pe an pentru a:

9.1.1 Verifica menținerea conformității cu ISO/IEC 27001, RGPD, NIS2 și DORA

9.1.2 Reflecta amenințările actualizate sau modificările celor mai bune practici de dezvoltare securizată

9.1.3 Asigura compatibilitatea cu orice instrumente, platforme sau relații cu furnizori noi

9.2 Revizuirile intermediare trebuie declanșate de:

9.2.1 Orice incident de securitate software raportat

9.2.2 Introducerea unui nou framework de dezvoltare sau a unei noi platforme de găzduire

9.2.3 O schimbare a partenerilor terți de dezvoltare

9.2.4 Actualizări de reglementare care afectează obligațiile privind software-ul sau securitatea

9.3 Toate modificările aduse acestei politici trebuie:

9.3.1 Să fie documentate cu data, rezumatul modificării și aprobarea GM

9.3.2 Să fie comunicate clar întregului personal intern și extern implicat în dezvoltare

9.3.3 Să fie păstrate ca parte a controlului versiunilor politicii și a istoricului modificărilor organizației

9.4 Versiunile actualizate trebuie puse la dispoziție într-un mod ușor accesibil, fie prin platforme interne, documentație tipărită sau servicii cloud accesibile furnizorilor.

10. Politici conexe și interdependențe

10.1 Această politică sprijină și depinde de implementarea cu succes a mai multor alte politici SME:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește răspunderea pentru alocarea și verificarea controalelor de securitate aferente dezvoltării în toate proiectele și la toți furnizorii.

10.1.2 P4S – Politica de control al accesului: stabilește regulile de bază pentru limitarea accesului la mediile de dezvoltare și la depozitele de cod, inclusiv separarea atribuțiilor.

10.1.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: asigură că dezvoltatorii interni și contractanții înțeleg practicile de programare securizată și responsabilitățile de securitate aferente.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: clarifică modul în care datele cu caracter personal trebuie gestionate în procesele de dezvoltare, testare și jurnalizare pentru a menține conformitatea cu RGPD.

10.1.5 P30S – Politica de răspuns la incidente: definește modul în care incidentele de securitate legate de dezvoltare trebuie raportate, evaluate și remediate, inclusiv expunerile legate de cod.

10.2 Aceste politici funcționează împreună pentru a asigura că dezvoltarea securizată este realizabilă și verificabilă, chiar și într-o organizație mică sau non-tehnică.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Impune implementarea controalelor operaționale, inclusiv dezvoltarea securizată, aliniate la obiectivele organizației și la profilul de risc.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.25 – Recomandă integrarea securității pe tot parcursul ciclului de viață al software-ului, inclusiv controlul codului-sursă, versionarea și accesul dezvoltatorilor.

11.2.2 Controlul 8.26 – Specifică metode pentru testarea aplicațiilor și verificarea funcționalităților de securitate înainte de intrarea în producție.

11.2.3 Controlul 8.27 – Impune ca dezvoltatorii terți să respecte aceleași standarde de dezvoltare și să aibă responsabilitățile de securitate clar definite.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 până la SA-15 – Definesc procese de dezvoltare securizată, inclusiv controlul accesului dezvoltatorilor, testarea, modelarea amenințărilor și documentarea.

11.3.2 SI-10 – Impune dezvoltatorilor să identifice și să atenueze punctele slabe comune ale software-ului și să utilizeze instrumente automatizate acolo unde este aplicabil.

11.4 RGPD al UE (2016/679)

11.4.1 Articolul 25 – „Protecția datelor încă din faza de proiectare și în mod implicit” impune integrarea măsurilor de securitate și de protecție a confidențialității în timpul proiectării și dezvoltării software-ului, în special atunci când sunt prelucrate date cu caracter personal.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(a), (e) și (h) – Impune politici de dezvoltare securizată, supravegherea utilizării componentelor open-source și atenuarea documentată a riscurilor asociate aplicațiilor în cadrul entităților esențiale și importante.

11.6 DORA a UE (2022/2554)

11.6.1 Articolele 6(7), 9(1)(c) și 10(2)(c) – Impun obligații de securitate pe ciclul de viață al dezvoltării pentru entitățile din sectorul financiar, inclusiv IMM-uri, în special pentru sistemele TIC critice.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build” sprijină implementarea unor controale de dezvoltare structurate care pun accent pe securitate, trasabilitate și reziliență, adaptate constrângerilor specifice IMM-urilor.