					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P25					Titlul documentului: **Politica privind cerințele de securitate a aplicațiilor**							
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	—
ISO/IEC 27002:2022	Controalele 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR	Articolele 25, 32	—
Directiva UE NIS2	Articolele 21(2)(f), 23	—
Regulamentul UE DORA	Articolele 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Scop

1.1 Această politică stabilește cerințele obligatorii de securitate la nivelul aplicațiilor pentru software-ul dezvoltat, achiziționat, integrat sau implementat de organizație. Aceasta asigură faptul că toate aplicațiile sunt proiectate, implementate și menținute în conformitate cu principiile dezvoltării securizate, obligațiile de reglementare și apetitul la risc al organizației.

1.2 Politica impune integrarea securității pe întreg ciclul de viață al aplicației, acoperind autentificarea utilizatorilor, gestionarea datelor, protecția interfețelor și interacțiunea securizată cu API-uri sau servicii.

1.3 Prin adoptarea acestei politici, organizația urmărește să prevină introducerea vulnerabilităților software, să protejeze datele sensibile și să asigure trasabilitatea și reziliența împotriva exploatării și utilizării abuzive.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor:

2.1.1 aplicațiilor dezvoltate intern sau obținute din surse externe, inclusiv soluțiilor SaaS și instrumentelor dezvoltate la comandă

2.1.2 aplicațiilor care susțin activități operaționale critice ale organizației, accesul clienților sau prelucrarea datelor reglementate

2.1.3 echipelor de dezvoltare, DevOps, QA, produs și securitate

2.1.4 dezvoltatorilor terți, furnizorilor de software și partenerilor de integrare care au acces la aplicațiile organizației sau la API-uri

2.2 Aceasta se aplică în toate mediile: dezvoltare, testare, preproducție, producție și recuperare în caz de dezastru, indiferent dacă sunt găzduite on-premises, în centre de date private sau în medii cloud publice.

3. Obiective

3.1 Să definească cerințe de securitate funcționale și nefuncționale de bază care trebuie îndeplinite de toate aplicațiile, indiferent de metoda de dezvoltare sau de stiva tehnologică.

3.2 Să asigure integrarea mecanismelor de protecție la nivelul aplicației, inclusiv validarea intrărilor, codificarea ieșirilor, tratarea erorilor și securitatea sesiunilor.

3.3 Să impună implementarea securizată a mecanismelor de autentificare, autorizare și control al accesului, aliniate cu politicile organizației privind identitatea și accesul.

3.4 Să impună interacțiunea securizată cu API-uri, interfețe web și componente terțe, utilizând protocoale aprobate și controale de securitate.

3.5 Să permită detectarea timpurie și atenuarea vulnerabilităților prin analiză statică și dinamică, revizuirea codului și modelarea amenințărilor.

3.6 Să protejeze datele sensibile în conformitate cu cerințele de reglementare prin aplicarea criptării, clasificării și regulilor de retenție a datelor.

3.7 Să asigure validarea continuă a profilului de risc al securității aplicațiilor după implementare, prin testare, monitorizare și pregătire pentru audit.

4. Roluri și responsabilități

4.1 Directorul pentru securitatea informațiilor (CISO)

4.1.1 Deține această politică și asigură alinierea acesteia la strategia de securitate a informațiilor și la profilul de risc al organizației.

4.1.2 Aprobă cerințele de securitate a aplicațiilor și impune controale obligatorii în cadrul funcțiilor de dezvoltare și achiziții.

4.2 Responsabilul cu securitatea aplicațiilor / Managerul DevSecOps

4.2.1 Definește controalele de securitate de bază și metodologiile de testare pentru componentele aplicației.

4.2.2 Asigură supravegherea integrării securizate a unor instrumente precum SAST, DAST, IAST și SCA în fluxul de livrare software.

4.2.3 Menține lista de verificare a cerințelor de securitate a aplicațiilor și criteriile de validare.

[... 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 notificări privind vulnerabilități critice care afectează frameworkuri sau dependențe utilizate pe scară largă

9.1.2 actualizări ale obligațiilor de reglementare privind securitatea aplicațiilor (de exemplu, NIS2, DORA)

9.1.3 schimbări majore în practicile de dezvoltare software, în instrumentele utilizate sau în arhitectura cloud a organizației

9.1.4 constatări rezultate din audituri interne sau teste externe de penetrare

9.2 Revizuirea trebuie coordonată de Responsabilul cu securitatea aplicațiilor, în colaborare cu CISO, responsabilii de inginerie DevOps, juridic, achiziții și QA.

9.3 Toate reviziile trebuie să fie supuse controlului versiunilor în registrul de control al documentelor SMSI și distribuite tuturor echipelor de dezvoltare și produs afectate.

9.4 Versiunile înlocuite trebuie arhivate pentru o perioadă de minimum trei ani, pentru trasabilitate, demonstrarea conformității și sprijinirea investigațiilor privind încălcarea securității.

10. Politici conexe și interdependențe

10.1 P1 – Politica de securitate a informațiilor. Stabilește baza pentru protejarea sistemelor și datelor, în cadrul căreia sunt necesare controale la nivelul aplicațiilor pentru prevenirea accesului neautorizat, a scurgerilor de date și a exploatării.

10.2 P4 – Politica de control al accesului. Definește standardele de management al identității și al sesiunilor care trebuie aplicate de toate aplicațiile, inclusiv autentificare puternică, principiul privilegiului minim și cerințe privind revizuirea drepturilor de acces.

10.3 P5 – Politica de management al schimbărilor. Reglementează promovarea codului aplicațiilor și a configurațiilor în mediile de producție, asigurând blocarea schimbărilor neautorizate sau netestate.

10.4 P17 – Politica de protecție a datelor și confidențialitate. Impune aplicațiilor să implementeze protecția datelor încă din faza de proiectare și să asigure gestionarea legală, criptarea și retenția datelor cu caracter personal și a datelor sensibile în toate mediile.

10.5 P24 – Politica privind dezvoltarea securizată. Oferă cadrul general pentru integrarea securității în SDLC, iar această politică stabilește cerințele concrete și controalele tehnice care trebuie implementate la nivelul aplicației.

10.6 P30 – Politica de răspuns la incidente. Impune tratarea structurată a incidentelor de securitate a aplicațiilor, inclusiv a vulnerabilităților identificate după implementare sau în timpul testării de penetrare, și stabilește procedurile de escaladare, limitare a impactului și recuperare.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:2022

11.1.1 Clauza 8.1 – Planificare și control operațional: impune integrarea securității aplicațiilor în procese și sisteme pentru a asigura confidențialitatea, integritatea și disponibilitatea (CIA).

11.2 ISO/IEC 27002:2022

11.2.1 Controalele 8.25–8.26: detaliază așteptările privind securitatea la nivelul aplicațiilor, inclusiv practici de programare securizată, modelarea amenințărilor, controale arhitecturale și validarea software-ului terț.

11.2.2 Anexa A Control 8.25 – Ciclul de viață al dezvoltării securizate: impune integrarea securității pe întreg ciclul de viață al aplicației.

11.2.3 Anexa A Control 8.26 – Cerințe de securitate a aplicațiilor: impune definirea și aplicarea controalelor tehnice pentru protejarea aplicațiilor împotriva utilizării abuzive și compromiterii.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Testarea și evaluarea securității realizate de dezvoltator: impune testare statică, dinamică și de penetrare în timpul dezvoltării.

11.3.2 SA-15 – Procesul de dezvoltare, standarde și instrumente: stabilește standarde formale pentru dezvoltarea securizată a aplicațiilor.

11.3.3 SI-10 – Validarea datelor de intrare ale informațiilor: impune mecanisme de control pentru prevenirea atacurilor de injecție și de parsare.

11.4 GDPR (UE) 2016/679

11.4.1 Articolul 25 – Protecția datelor începând cu momentul conceperii și în mod implicit: impune integrarea protecției datelor și a confidențialității în logica aplicației și în fluxurile de lucru.

11.4.2 Articolul 32 – Securitatea prelucrării: impune măsuri tehnice adecvate, precum validarea intrărilor, criptarea și controale de acces securizate.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolul 21(2)(f): impune tratarea vulnerabilităților și practici securizate privind ciclul de viață al aplicațiilor pentru entitățile esențiale și importante.

11.5.2 Articolul 23 – Raportarea incidentelor de securitate: necesită capabilități de jurnalizare și monitorizare la nivelul aplicațiilor pentru detectarea și raportarea incidentelor semnificative.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: obligă entitățile financiare să asigure că aplicațiile sunt securizate, testate și reziliente la amenințări cibernetice.

11.6.2 Articolul 11 – Testarea instrumentelor TIC: încurajează testarea periodică de penetrare și exerciții de tip red team pentru aplicațiile și serviciile critice.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionarea identificării și dezvoltării soluțiilor: stabilește cerințe de proiectare și control în timpul dezvoltării aplicațiilor.

11.7.2 BAI09 – Gestionarea aplicațiilor: pune accent pe mentenanța securizată, monitorizarea și îmbunătățirea aplicațiilor aflate în exploatare.

11.7.3 DSS05 – Gestionarea serviciilor de securitate: corelează protecția aplicațiilor cu operațiunile și controalele de securitate mai largi ale organizației.