					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P25S					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	Controale operaționale, inclusiv securitatea aplicațiilor
ISO/IEC 27002:2022	Controalele 8.25–8.26	Proiectare securizată, dezvoltare, testare și revizuire a codului
NIST SP 800-53 Rev.5	SA-11, SI-10	Testarea aplicațiilor de către dezvoltatori, analiza codului, prevenirea defectelor
GDPR al UE	Articolul 25	Protecția datelor începând cu faza de proiectare și în mod implicit
Directiva NIS2 a UE	Articolul 21(2)(a), (e)	Măsuri tehnice pentru securizarea aplicațiilor și detectarea riscurilor
Regulamentul DORA al UE	Articolele 9(2)(c), 10(2)(c)	Securitatea aplicațiilor pentru reziliența operațională digitală
COBIT 2019	BAI03	Gestionarea dezvoltării/achiziției de software securizat

1. Scop

1.1 Prezenta politică definește controalele minime obligatorii de securitate a aplicațiilor necesare pentru toate soluțiile software și de sistem utilizate de organizație, indiferent dacă sunt dezvoltate intern sau achiziționate de la furnizori externi.

1.2 Aceasta asigură că aplicațiile sunt proiectate, implementate și menținute astfel încât să protejeze datele clienților, ale angajaților și datele organizației împotriva accesului neautorizat, utilizării necorespunzătoare, modificării sau distrugerii.

1.3 Prezenta politică sprijină eforturile organizației de a obține și menține certificarea ISO/IEC 27001, de a respecta obligațiile GDPR și NIS2 și de a reduce riscurile operaționale asociate implementărilor software nesecurizate.

1.4 Aceasta contribuie la crearea unei abordări consecvente și verificabile privind securitatea aplicațiilor pentru IMM-uri, prin stabilirea unei liste unitare de verificare a caracteristicilor și practicilor de securitate, adaptată pentru medii cu resurse tehnice interne limitate.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor aplicațiilor, sistemelor, instrumentelor și platformelor care:

2.1.1 Sunt dezvoltate intern, personalizate sau realizate prin scripturi pentru uz intern

2.1.2 Sunt achiziționate ca software comercial, SaaS sau sisteme bazate pe cloud

2.1.3 Prelucrează, stochează sau transmit date cu caracter personal, înregistrări de afaceri sau informații operaționale sensibile

2.1.4 Sunt accesate de angajați, contractori, clienți sau parteneri prin rețele interne, internet sau platforme mobile

2.2 Politica acoperă:

2.2.1 Dezvoltatorii (interni sau contractați)

2.2.2 Furnizorii de software și furnizorii de servicii cloud

2.2.3 Personalul de suport IT sau administratorii responsabili de implementare și suport

2.2.4 Proprietarii de aplicații și utilizatorii din business implicați în aprobarea și supravegherea sistemelor

3. Obiective

3.1 Să asigure că toate aplicațiile utilizate de organizație includ controale de securitate integrate și verificabile, care reduc vulnerabilitățile software uzuale.

3.2 Să protejeze confidențialitatea, integritatea și disponibilitatea datelor prelucrate de aplicații, indiferent de locul în care acestea sunt găzduite.

3.3 Să impună testarea, revizuirea și validarea formală a securității aplicațiilor înainte ca orice aplicație nouă sau actualizare majoră să fie aprobată pentru utilizare în producție.

3.4 Să permită gestionarea consecventă și securizată a acreditărilor utilizatorilor, a datelor de sesiune și a drepturilor de acces în toate sistemele critice pentru activitățile organizației.

3.5 Să impună funcționalități de jurnalizare securizată, capabilități de audit și funcții de monitorizare în toate aplicațiile pentru a sprijini detectarea și răspunsul la activități suspecte.

3.6 Să reducă riscurile juridice și de conformitate prin asigurarea faptului că aplicațiile respectă cerințele de securitate de reglementare aplicabile.

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Deține responsabilitatea generală pentru securitatea aplicațiilor la nivelul întregii organizații.

4.1.2 Aprobă prezenta politică și se asigură că toate achizițiile sau proiectele de dezvoltare respectă cerințele acesteia.

4.1.3 Se asigură că furnizorii și prestatorii de servicii au obligația contractuală de a respecta cerințele de securitate a aplicațiilor.

4.1.4 Revizuiește și aprobă excepțiile de risc atunci când conformitatea deplină nu poate fi atinsă din cauza unor constrângeri de business.

4.2 Proprietar de aplicație (dacă este desemnat)

4.2.1 Identifică nevoile specifice de securitate ale aplicației în timpul selecției sistemului sau la inițierea proiectului.

4.2.2 Verifică includerea funcționalităților esențiale, precum protecția autentificării, criptarea și jurnalizarea activităților.

4.2.3 Participă la revizuirile premergătoare implementării și confirmă că controalele de securitate răspund nevoilor de business.

[... 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 de Directorul general cel puțin o dată în fiecare an calendaristic pentru a:

9.1.1 Reflecta modificările cerințelor de reglementare (de exemplu, GDPR, NIS2, DORA)

9.1.2 Include amenințări și tehnici de atac noi sau emergente

9.1.3 Actualiza formularile și cerințele pentru a reflecta schimbările privind platformele, furnizorii sau metodele de dezvoltare

9.2 De asemenea, trebuie efectuate revizuiri intermediare atunci când:

9.2.1 Sunt introduse aplicații noi

9.2.2 Aplicațiile existente sunt supuse unor actualizări sau integrări semnificative

9.2.3 Are loc un incident sau o încălcare a securității legată de o aplicație

9.2.4 Sunt identificate riscuri noi din informări externe sau alerte din industrie

9.3 Toate actualizările aduse prezentei politici trebuie:

9.3.1 Să fie aprobate de Directorul general

9.3.2 Să fie documentate cu istoricul versiunilor și motivul modificării

9.3.3 Să fie comunicate tuturor angajaților, dezvoltatorilor și furnizorilor implicați în administrarea aplicațiilor

9.3.4 Să fie stocate în condiții de securitate pentru referințe de audit și conformitate

10. Politici conexe și interdependențe

10.1 Prezenta politică este susținută direct de următoarele politici de securitate aliniate pentru IMM-uri și contribuie la aplicarea acestora:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: Atribuie responsabilitatea pentru aprobarea aplicațiilor, aplicarea politicii și managementul furnizorilor.

10.1.2 P4S – Politica de control al accesului: Asigură că accesul la aplicații este aliniat cu principiul privilegiului minim și cu principiile de control al sesiunilor.

10.1.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: Asigură că utilizatorii și dezvoltatorii sunt instruiți să recunoască și să raporteze amenințările legate de aplicații.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: Stabilește măsurile de protecție a confidențialității datelor care trebuie aplicate de orice aplicație care prelucrează date cu caracter personal.

10.1.5 P14S – Politica de păstrare și eliminare a datelor: Reglementează modul în care jurnalele, backup-urile și datele sensibile generate de aplicații trebuie păstrate, arhivate și distruse în condiții de securitate.

10.1.6 P30S – Politica de răspuns la incidente: Descrie pașii pentru identificarea, raportarea și limitarea impactului evenimentelor de securitate legate de aplicații.

10.2 Împreună, aceste politici asigură integrarea deplină a securității aplicațiilor în Sistemul de management al securității informației (SMSI) al organizației și menținerea pregătirii pentru audit.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Impune organizațiilor să stabilească controale operaționale pentru tratarea riscurilor de securitate a informației, inclusiv a celor legate de aplicații și sisteme software.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.25 – Recomandă implementarea practicilor de proiectare securizată, dezvoltare securizată și revizuire a codului pentru toate aplicațiile, inclusiv pentru cele furnizate de terți.

11.2.2 Controlul 8.26 – Recomandă testarea formală a controalelor de securitate ale aplicațiilor, în special în domenii care implică controlul accesului, validarea datelor de intrare și gestionarea sesiunilor.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Specifică cerințe pentru testarea de către dezvoltatori, analiza codului și scanarea dinamică a aplicațiilor înainte de implementare.

11.3.2 SI-10 – Vizează detectarea și prevenirea defectelor software uzuale, cu accent pe conștientizarea dezvoltatorilor și pe măsuri tehnice de protecție.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 25 – „Protecția datelor începând cu faza de proiectare și în mod implicit” impune integrarea confidențialității și securității în proiectarea de bază a aplicațiilor care prelucrează date cu caracter personal.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(a) și (e) – Impune entităților esențiale și importante să implementeze măsuri tehnice pentru securizarea aplicațiilor și detectarea riscurilor legate de software.

11.6 DORA a UE (2022/2554)

11.6.1 Articolul 9(2)(c), 10(2)(c) – Impune IMM-urilor din sectorul financiar să integreze controale de securitate la nivel de aplicație și să efectueze evaluări periodice pentru menținerea rezilienței operaționale digitale.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build” oferă îndrumări pentru dezvoltarea sau achiziția de software securizat, aliniat la risc, conformitate și cerințele de business, inclusiv în medii IMM cu resurse limitate.