					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P28S					Titlul documentului: **Politica privind dezvoltarea externalizată**							
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	Clauzele 5.1, 6.1, 8	Controale aplicabile SMSI și controale referitoare la furnizori
ISO/IEC 27002:2022	Controalele 5.19, 5.20, 8.25–8.27	Controale privind furnizorii și ciclul de viață al dezvoltării securizate
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Cerințe privind achiziția, lanțul de aprovizionare, dezvoltarea securizată și acordurile cu furnizorii
GDPR	Articolul 28	Cerințe contractuale și de protecție a datelor pentru prelucrarea efectuată de terți
Directiva NIS2	Articolul 21(2)(a), (h)	Controale privind lanțul de aprovizionare și dezvoltarea securizată a aplicațiilor
Regulamentul DORA	Articolul 10	Managementul riscurilor asociate terților TIC, inclusiv dezvoltarea externalizată
COBIT 2019	BAI03, DSS05	Cerințe pentru dezvoltarea externă și furnizorii externi de servicii IT

1. Scop

1.1 Prezenta politică asigură că întreaga dezvoltare software externalizată — indiferent dacă este realizată de freelanceri, agenții sau furnizori terți — se desfășoară în condiții de securitate, sub control contractual și în conformitate cu cerințele legale, de reglementare și de audit aplicabile.

1.2 Aceasta protejează organizația împotriva riscurilor asociate codului nesecurizat, drepturilor de proprietate neclare, expunerii datelor și managementului necorespunzător al furnizorilor, prin impunerea unor standarde de dezvoltare aplicabile și a supravegherii furnizorilor, inclusiv în absența unui departament IT dedicat.

1.3 Prezenta politică sprijină certificarea ISO/IEC 27001:2022 prin definirea clară a cerințelor privind dezvoltarea, a responsabilităților și a controalelor documentate aplicabile activităților de dezvoltare efectuate de terți.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică următoarelor:

2.1.1 tuturor dezvoltatorilor externalizați, inclusiv freelancerilor și agențiilor de dezvoltare

2.1.2 oricărei activități de dezvoltare care implică instrumente interne, site-uri web publice, aplicații software sau automatizarea activităților organizației

2.1.3 personalului responsabil cu selectarea, gestionarea sau supravegherea dezvoltatorilor externi

2.1.4 oricărei integrări de sisteme realizate de terți, activități de scripting sau dezvoltări care interacționează cu datele sau sistemele companiei

2.2 Domeniul de aplicare include, de asemenea, orice parte sau platformă care are acces la credențialele companiei, depozite de date, depozite de cod sursă, medii de testare intermediară sau sisteme de producție.

3. Obiective

3.1 Să asigure că întreaga dezvoltare externalizată respectă principiile programării securizate și că dezvoltatorii au obligații contractuale de a respecta standardele documentate și clauzele de confidențialitate.

3.2 Să stabilească dreptul de proprietate asupra tuturor livrabilelor — cod, active, credențiale și documentație — asigurând transferul integral al drepturilor către companie și predarea trasabilă la finalizarea proiectului.

3.3 Să prevină riscurile uzuale asociate dezvoltării, inclusiv reutilizarea codului proprietar, atacurile asupra lanțului de aprovizionare prin biblioteci, utilizarea de framework-uri neacceptate și accesul administrativ neverificat.

3.4 Să impună documentația prealabilă pentru fiecare proiect externalizat, inclusiv contracte, acorduri de confidențialitate (NDA) și cerințe minime de securitate.

3.5 Să protejeze datele clienților, sistemele și procesele interne prin aplicarea unei supravegheri riguroase a dezvoltării, a testării după livrare și a managementului securizat al accesului la sisteme.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Aprobă toate relațiile cu furnizorii și semnează acordurile de dezvoltare.

4.1.2 Se asigură că întreaga dezvoltare externalizată respectă prezenta politică.

4.1.3 Revocă accesul la sistemele companiei după finalizarea proiectului.

4.1.4 Revizuiește documentația și rezultatele post-livrare.

4.2 Responsabil de proiect (de regulă, angajat intern sau coordonator desemnat)

4.2.1 Gestionează coordonarea curentă cu dezvoltatorul extern.

4.2.2 Verifică îndeplinirea cerințelor funcționale și testarea livrabilelor.

4.2.3 Se asigură de predarea securizată a codului și a credențialelor.

4.2.4 Raportează Directorului general orice problemă sau incident legat de dezvoltare.

[... 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 Revizuire anuală

9.1.1 Prezenta politică trebuie revizuită de Directorul general cel puțin o dată pe an. Revizuirea asigură că aceasta continuă să îndeplinească:

9.1.1.1 cerințele pentru certificarea ISO/IEC 27001

9.1.1.2 modificările obligațiilor legale (de exemplu, articolul 28 din GDPR, articolul 10 din DORA)

9.1.1.3 practicile curente de dezvoltare la nivelul IMM-urilor și riscurile asociate terților

9.2 Revizuiri intermediare

9.2.1 Revizuirea politicii trebuie realizată și atunci când:

9.2.1.1 este integrat un nou furnizor sau o nouă platformă pentru dezvoltare externalizată

9.2.1.2 are loc un incident semnificativ care implică dezvoltarea externalizată

9.2.1.3 apar modificări semnificative ale instrumentelor, platformelor sau mediilor utilizate

9.3 Procesul de revizuire

9.3.1 Directorul general este responsabil pentru:

9.3.1.1 verificarea faptului că procesele privind contractele, acordurile de confidențialitate (NDA) și controlul accesului rămân eficace

9.3.1.2 confirmarea faptului că furnizorii actuali și freelancerii sunt aliniați la politică

9.3.1.3 revizuirea prevederilor pe baza feedbackului din proiecte sau a incidentelor anterioare

9.4 Controlul versiunilor și comunicare

9.4.1 Toate modificările trebuie:

9.4.1.1 înregistrate împreună cu data, motivul și descrierea modificării

9.4.1.2 aprobate de Directorul general și adăugate în istoricul versiunilor

9.4.1.3 comunicate întregului personal sau responsabililor de proiect care lucrează cu dezvoltatori externi

9.4.1.4 redistribuite tuturor furnizorilor și terților afectați, atunci când este necesar

10. Politici conexe și interdependențe

10.1 Prezenta politică sprijină în mod direct și depinde de implementarea următoarelor politici aliniate pentru IMM-uri:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: clarifică responsabilitățile privind aprobarea furnizorilor, controlul accesului și acceptarea riscurilor atunci când sunt utilizați dezvoltatori externalizați.

10.1.2 P4S – Politica de control al accesului: definește crearea, restricționarea și încetarea corespunzătoare a conturilor de utilizator și a accesului administrativ utilizate în dezvoltarea externalizată.

10.1.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: asigură că personalul intern înțelege cum să coordoneze în condiții de securitate activitatea cu dezvoltatorii externi, inclusiv gestionarea credențialelor și a fișierelor de proiect.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: stabilește cerințele de securitate și legale pentru gestionarea datelor cu caracter personal care pot fi prelucrate de dezvoltatori externalizați în temeiul GDPR.

10.1.5 P24S – Politica de dezvoltare securizată: specifică modul în care dezvoltarea internă și externă trebuie să respecte practicile de programare securizată și verificarea bibliotecilor și a framework-urilor.

10.1.6 P30S – Politica de răspuns la incidente: este necesară atunci când dezvoltarea externalizată conduce la incidente de securitate sau vulnerabilități, orientând investigarea și remedierea coordonată.

10.2 Aceste politici trebuie implementate în paralel pentru a se asigura că dezvoltarea externalizată nu generează riscuri necontrolate și nu conduce la nerespectarea obligațiilor de conformitate aplicabile IMM-urilor.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1 – Organizațiile trebuie să evalueze și să trateze riscurile de securitate a informației asociate furnizorilor.

11.1.2 Clauza 8.1 – Impune planificarea și controlul operațional, inclusiv pentru servicii prestate de terți, cum ar fi dezvoltarea externalizată.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.19 – Recomandă evaluarea capacității furnizorilor de a îndeplini cerințele de securitate a informației.

11.2.2 Controlul 5.20 – Încurajează monitorizarea și revizuirea periodică a serviciilor prestate de terți.

11.2.3 Controalele 8.25–8.27 – Descriu practici privind ciclul de viață al dezvoltării securizate aplicabile dezvoltării externalizate.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-4 – Impune includerea măsurilor de securitate a informației în strategiile de achiziție.

11.3.2 SA-9 – Abordează dezvoltarea sistemelor externe și riscurile asociate lanțului de aprovizionare.

11.3.3 SA-11 – Definește practici de dezvoltare securizată, inclusiv revizuirea codului și remedierea defectelor.

11.3.4 SA-15 – Încurajează utilizarea instrumentelor automatizate pentru detectarea defectelor și asigurarea software-ului.

11.3.5 SR-3 – Impune includerea cerințelor de securitate cibernetică în acordurile cu furnizorii.

11.4 Regulamentul general privind protecția datelor (GDPR)

11.4.1 Articolul 28 – Impune încheierea de contracte cu persoane împuternicite terțe pentru a asigura măsuri de protecție adecvate pentru date, fiind direct aplicabil dezvoltatorilor care prelucrează sau accesează date cu caracter personal.

11.5 Directiva NIS2 (UE) 2022/2555

11.5.1 Articolul 21(2)(a), (h) – Impune controale de securitate pentru lanțul de aprovizionare și practici de dezvoltare software securizată pentru furnizorii de servicii digitale aflați în domeniul de aplicare, inclusiv pentru IMM-uri, după caz.

11.6 Regulamentul DORA

11.6.1 Articolul 10 – Impune managementul riscurilor asociate terților TIC, inclusiv acorduri de dezvoltare, obligații de securitate și controale de risc referitoare la furnizori terți.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionarea identificării și dezvoltării soluțiilor – asigură că dezvoltarea externă îndeplinește cerințele organizației și așteptările de securitate.

11.7.2 DSS05 – Gestionarea serviciilor de securitate – impune ca serviciile externe de securitate și furnizorii de dezvoltare să opereze în baza unor reguli de securitate aplicate și sub supraveghere.