					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P28					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**

Notă juridică (drepturi de autor și restricții de utilizare)

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8.1	N/A
ISO/IEC 27002:2022	Controalele 5.19-5.22, 8	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
GDPR	Articolele 28, 32	N/A
Directiva NIS2	Articolele 21(2)(a), (h), 23	N/A
Regulamentul DORA	Articolele 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Scop

1.1 Această politică definește controalele obligatorii pentru externalizarea dezvoltării de software sau sisteme către furnizori externi, contractori sau agenții, asigurând integrarea practicilor de dezvoltare securizată pe întreg ciclul de viață al dezvoltării.

1.2 Scopul acesteia este de a preveni vulnerabilitățile de securitate, pierderea datelor, expunerea proprietății intelectuale (IP) și încălcările de conformitate rezultate din activitățile de dezvoltare externalizată.

1.3 Politica stabilește cerințe privind guvernanța furnizorilor, standardele de programare securizată, managementul accesului, obligațiile de monitorizare și încetarea colaborării la finalul contractului, pentru a menține confidențialitatea, integritatea și disponibilitatea (CIA) software-ului dezvoltat.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor unităților organizaționale care implică entități externe în dezvoltarea de software sau sisteme, inclusiv:

2.1.1 aplicații web, aplicații mobile, sisteme embedded, API-uri, scripturi, fluxuri de automatizare sau module de platformă

2.1.2 dezvoltare personalizată pentru platforme interne, sisteme destinate clienților sau produse comerciale

2.1.3 colaborări cu dezvoltatori terți, freelanceri, agenții sau echipe offshore

2.2 Politica reglementează, de asemenea, orice entitate externă care accesează codul sursă, mediile de testare sau fluxurile de integrare și livrare continuă (CI/CD) pe durata dezvoltării.

2.3 Cerințele sunt obligatorii indiferent de tipul contractului, metodologia de dezvoltare sau locația geografică a furnizorului externalizat.

3. Obiective

3.1 Să impună practici de dezvoltare securizată pe ciclul de viață al dezvoltării (SDLC) în toate colaborările externalizate, de la planificare până la validarea post-implementare.

3.2 Să asigure că toate contractele cu dezvoltatori externi includ clauze obligatorii privind protecția datelor, programarea securizată și menținerea drepturilor de proprietate intelectuală.

3.3 Să definească cerințele privind controlul accesului, monitorizarea și auditul pentru dezvoltatorii terți care interacționează cu sistemele interne.

3.4 Să protejeze organizația împotriva amenințărilor din lanțul de aprovizionare, încălcărilor legale și prejudiciilor reputaționale asociate software-ului dezvoltat extern.

3.5 Să mențină conformitatea continuă cu cadrele de securitate aplicabile, inclusiv ISO/IEC 27001, NIST, GDPR, NIS2, DORA și COBIT 2019.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă proiectele de dezvoltare externalizată cu risc ridicat și validează excepțiile de la politică atunci când acestea sunt justificate.

4.1.2 Asigură alinierea deciziilor de externalizare la obiectivele strategice și la apetitul la risc al organizației.

4.2 Directorul de securitate a informațiilor (CISO)

4.2.1 Aprobă integrarea furnizorilor din perspectiva securității.

4.2.2 Definește cerințele privind controalele de securitate pentru colaborările externalizate și revizuiește rapoartele de incident.

[... 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 cel puțin anual sau mai frecvent în următoarele situații:

9.1.1 introducerea unor noi modele de externalizare a dezvoltării, a unor noi furnizori sau a unor noi jurisdicții

9.1.2 actualizări ale cadrelor de reglementare, precum GDPR, NIS2 sau DORA

9.1.3 în urma unui incident de securitate care implică cod externalizat, acces sau livrabile

9.1.4 ca parte a constatărilor auditului intern sau a îmbunătățirilor aduse SMSI

9.2 Directorul de securitate a informațiilor (CISO) este responsabil de inițierea și coordonarea revizuirii politicii, în consultare cu:

9.2.1.1 funcția juridică și Achiziții (pentru alinierea aplicării contractuale)

9.2.1.2 proprietarii de proiect și de produs (pentru fezabilitatea operațională)

9.2.1.3 echipa de securitate a informațiilor (pentru actualizări privind amenințările și controalele)

9.2.1.4 managementul executiv (pentru aprobarea finală)

9.3 Toate actualizările politicii trebuie:

9.3.1.1 să facă obiectul controlului versiunilor și să fie stocate într-un depozit de documente desemnat

9.3.1.2 să fie comunicate părților interesate implicate în activități de dezvoltare externalizată

9.3.1.3 să fie corelate cu orice actualizări ale politicilor conexe sau ale documentației procedurale

9.4 Un registru al schimbărilor trebuie să însoțească fiecare versiune a politicii pentru a asigura trasabilitatea modificărilor și aprobărilor.

10. Politici conexe și interdependențe

10.1 Această politică susține și este susținută de următoarele documente conexe:

10.1.1 P1 - Politica de securitate a informației: stabilește principiile de securitate la nivel organizațional care se aplică în contexte de dezvoltare internă și realizată de terți.

10.1.2 P5 - Politica de management al schimbărilor: asigură că toate schimbările de implementare provenite din baze de cod externalizate sunt revizuite și aprobate înainte de punerea în producție.

10.1.3 P13 - Politica de clasificare și etichetare a datelor: stabilește modul în care datele sensibile sunt identificate înainte de a fi expuse furnizorilor de dezvoltare sau depozitelor de cod.

10.1.4 P18 - Politica privind controalele criptografice: stabilește modul în care cheile, secretele și acreditările sensibile trebuie gestionate în timpul dezvoltării și livrării.

10.1.5 P24 - Politica de dezvoltare securizată: definește cerințele de bază pentru practicile de dezvoltare software internă și externă.

10.1.6 P30 - Politica de răspuns la incidente: reglementează modul în care încălcările sau problemele de securitate care implică dezvoltare externalizată sunt escaladate, investigate și soluționate.

10.1.7 P33 - Politica de audit și monitorizare a conformității: stabilește cerințele pentru revizuirea activităților de dezvoltare externalizată în timpul auditurilor sau al evaluărilor de conformitate.

11. Standarde și cadre de referință

11.1 Această politică este aliniată la cadre de securitate și reglementări recunoscute la nivel internațional, pentru a asigura externalizarea în condiții de securitate a dezvoltării software și practici adecvate de management al furnizorilor.

11.2 ISO/IEC 27001

11.2.1 Clauza 8.1 - Planificare și control operațional: impune controale de proces pentru dezvoltarea securizată și livrarea de către terți.

11.3 ISO/IEC 27002:2022 - Controalele 5.19-5.21, 8.

11.3.1 Anexa A, controlul 5.19 - managementul relațiilor cu furnizorii: impune acorduri formale cu clauze privind securitatea și conformitatea.

11.3.2 Anexa A, controlul 5.20 - abordarea securității informației în acordurile cu furnizorii: asigură integrarea în contracte a controalelor specifice dezvoltării.

11.3.3 Anexa A, controlul 5.21 - managementul livrării serviciilor furnizorilor: include monitorizarea livrabilelor și a riscurilor aferente dezvoltării realizate de terți.

11.3.4 Anexa A, controlul 8.27 - dezvoltare externalizată: impune cerințe de securitate definite și control al accesului pentru software-ul dezvoltat extern.

11.3.5 Aceste controale stabilesc cerințe structurate pentru selectarea, contractarea și supravegherea dezvoltatorilor externalizați, inclusiv practici de dezvoltare securizată, gestionarea codului și validarea performanței.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - procesul de achiziție: impune definirea cerințelor de dezvoltare securizată la momentul achiziției.

11.4.2 SA-9 - servicii de sisteme externe: reglementează modul în care dezvoltatorii terți interacționează în mod securizat cu serviciile interne.

11.4.3 SA-10 - managementul configurației dezvoltatorului: este aliniat cu obligațiile privind controlul versiunilor, accesul la cod și trasabilitatea schimbărilor pentru echipele externe.

11.5 GDPR (UE) 2016/679

11.5.1 Articolul 28 - obligațiile persoanei împuternicite: impune ca în contractele cu dezvoltatori terți să fie specificate cerințe de securitate, control și audit pentru gestionarea datelor cu caracter personal.

11.5.2 Articolul 32 - securitatea prelucrării: impune măsuri de protecție adecvate (de exemplu, criptare, controlul accesului) atunci când sunt dezvoltate sisteme care prelucrează date cu caracter personal.

11.6 Directiva NIS2 (UE) 2022/2555

11.6.1 Articolele 21(2)(a), (h), 23: impun aplicarea practicilor de dezvoltare securizată în toate colaborările cu terți și în lanțurile digitale de aprovizionare, cu supraveghere și verificare tehnică.

11.7 Regulamentul DORA (UE) 2022/2554

11.7.1 Articolele 28(1), (2): impun entităților financiare să gestioneze riscul TIC asociat terților prin controale contractuale și supravegherea dezvoltării securizate, în special pentru dezvoltarea externalizată critică.

11.8 COBIT 2019

11.8.1 APO10 - managementul furnizorilor: stabilește cerințe structurate pentru evaluarea furnizorilor, contracte și monitorizarea performanței.

11.8.2 BAI03 - managementul dezvoltării soluțiilor: corespunde direct proceselor SDLC securizate, revizuirilor de cod și validării dezvoltării.

11.8.3 DSS05 - managementul serviciilor de securitate: este aliniat cu monitorizarea și protecția sistemelor dezvoltate extern sau de către terți.