					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P28S					Naziv dokumenta: **Politika razvoja po narudžbi putem vanjskih pružatelja usluga**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađenost sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 6.1, 8	Primjenjive kontrole ISMS-a i kontrole povezane s dobavljačima
ISO/IEC 27002:2022	Kontrole 5.19, 5.20, 8.25–8.27	Kontrole dobavljača i kontrole životnog ciklusa sigurnog razvoja
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Zahtjevi za nabavu, opskrbni lanac, siguran razvoj i ugovore s dobavljačima
GDPR EU	Članak 28	Ugovorni zahtjevi i zahtjevi zaštite podataka za obradu koju provode treće strane
Direktiva NIS2 EU	Članak 21(2)(a), (h)	Kontrole sigurnosti opskrbnog lanca i sigurnog razvoja aplikacija
Uredba DORA EU	Članak 10	Upravljanje rizicima IKT-a povezanima s trećim stranama, uključujući izdvojeni razvoj
COBIT 2019	BAI03, DSS05	Zahtjevi za vanjski razvoj i vanjske pružatelje IS usluga

1. Svrha

1.1 Ova politika osigurava da se sav razvoj softvera povjeren vanjskim izvođačima — bilo da ga obavljaju freelanceri, agencije ili pružatelji usluga trećih strana — provodi na siguran način, uz odgovarajuće ugovorne kontrole i u skladu s primjenjivim pravnim, regulatornim i revizijskim zahtjevima.

1.2 Ova politika štiti organizaciju od rizika povezanih s nesigurnim kodom, nejasnim vlasništvom, izloženošću podataka i neadekvatnim upravljanjem dobavljačima uspostavom obvezujućih razvojnih standarda i nadzora nad dobavljačima, čak i kada ne postoji namjenski IT odjel.

1.3 Ova politika podupire certifikaciju prema normi ISO/IEC 27001:2022 uspostavom jasno definiranih očekivanja za razvoj, odgovornosti i dokumentiranih kontrola nad razvojnim aktivnostima koje provode treće strane.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 sve vanjske razvojne inženjere, uključujući freelancere i razvojne agencije

2.1.2 sve razvojne aktivnosti koje uključuju interne alate, javno dostupne mrežne stranice, softverske aplikacije ili poslovnu automatizaciju

2.1.3 osoblje odgovorno za odabir, upravljanje ili nadzor vanjskih razvojnih inženjera

2.1.4 svaku integraciju sustava treće strane, skriptiranje ili razvoj koji je u interakciji s podacima ili sustavima organizacije

2.2 Ova politika obuhvaća i svaku stranu ili platformu s pristupom vjerodajnicama organizacije, repozitorijima podataka, repozitorijima izvornog koda, testnim okruženjima ili produkcijskim sustavima.

3. Ciljevi

3.1 Osigurati da se sav razvoj koji provode vanjski izvođači odvija u skladu s praksama sigurnog kodiranja te da su razvojni inženjeri ugovorno obvezani primjenjivati dokumentirane standarde i odredbe o povjerljivosti.

3.2 Uspostaviti vlasništvo nad svim isporukama — kodom, imovinom, vjerodajnicama i dokumentacijom — uz osiguravanje potpunog prijenosa prava na organizaciju i sljedive primopredaje po završetku projekta.

3.3 Spriječiti uobičajene razvojne rizike, uključujući ponovnu uporabu vlasničkog koda, napade na opskrbni lanac putem biblioteka, uporabu nepodržanih razvojnih okvira i neprovjeren administratorski pristup.

3.4 Zahtijevati dokumentaciju prije početka angažmana za svaki projekt povjeren vanjskim izvođačima, uključujući ugovore, ugovore o povjerljivosti i minimalna sigurnosna očekivanja.

3.5 Zaštititi podatke klijenata, sustave i interne procese provedbom odgovarajućeg nadzora nad razvojem, testiranja nakon isporuke i sigurnog upravljanja pristupom sustavima.

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 Odobrava sve odnose s dobavljačima i potpisuje ugovore o razvoju.

4.1.2 Osigurava da se sav razvoj koji provode vanjski izvođači odvija u skladu s ovom politikom.

4.1.3 Ukida pristup sustavima organizacije po završetku projekta.

4.1.4 Pregledava dokumentaciju i rezultate nakon isporuke.

4.2 Vlasnik projekta (obično interni zaposlenik ili imenovani koordinator)

4.2.1 Upravlja svakodnevnom koordinacijom s vanjskim razvojnim inženjerom.

4.2.2 Provjerava jesu li funkcionalni zahtjevi ispunjeni i jesu li isporuke testirane.

4.2.3 Osigurava sigurnu isporuku koda i vjerodajnica.

4.2.4 Prijavljuje GM-u sve probleme ili incidente povezane s razvojem.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled

9.1.1 Ovu politiku mora pregledati glavni direktor (GM) najmanje jednom godišnje. Pregled osigurava da politika i dalje ispunjava:

9.1.1.1 zahtjeve za certifikaciju prema normi ISO/IEC 27001

9.1.1.2 promjene pravnih obveza (npr. članak 28. GDPR-a, članak 10. Uredbe DORA EU)

9.1.1.3 aktualne razvojne prakse na razini SME-a i rizike povezane s trećim stranama

9.2 Izvanredni pregledi

9.2.1 Pregledi politike moraju se provoditi i kada:

9.2.1.1 se uvodi novi dobavljač ili platforma za razvoj vanjskih izvođača

9.2.1.2 nastane značajan incident povezan s razvojem vanjskih izvođača

9.2.1.3 dođe do značajnih promjena u korištenim alatima, platformama ili okruženjima

9.3 Postupak pregleda

9.3.1 GM je odgovoran za:

9.3.1.1 provjeru da ugovori, ugovori o povjerljivosti i procesi kontrole pristupa ostaju djelotvorni

9.3.1.2 potvrdu da su postojeći dobavljači i freelanceri usklađeni s politikom

9.3.1.3 izmjenu odredbi na temelju povratnih informacija iz prethodnih projekata ili incidenata

9.4 upravljanje verzijama i komunikacija

9.4.1 Sve promjene moraju biti:

9.4.1.1 evidentirane s datumom, razlogom i opisom promjene

9.4.1.2 odobrene od strane GM-a i unesene u povijest verzija

9.4.1.3 priopćene svom osoblju ili vlasnicima projekata koji rade s vanjskim razvojnim inženjerima

9.4.1.4 ponovno distribuirane svim pogođenim dobavljačima i trećim stranama kada je to potrebno

10. Povezane politike i poveznice

10.1 Ova politika izravno podupire i ovisi o provedbi sljedećih politika usklađenih s potrebama SME-a:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: pojašnjava tko je odgovoran za odobravanje dobavljača, kontrolu pristupa i prihvaćanje rizika pri korištenju vanjskih razvojnih inženjera.

10.1.2 P4S – Politika kontrole pristupa: definira pravilno otvaranje, ograničavanje i ukidanje korisničkih računa i administratorskog pristupa koji se koriste tijekom razvoja vanjskih izvođača.

10.1.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da interno osoblje razumije kako sigurno koordinirati s vanjskim razvojnim inženjerima, uključujući postupanje s vjerodajnicama i projektnim datotekama.

10.1.4 P17S – Politika zaštite podataka i privatnosti: uspostavlja sigurnosne i pravne zahtjeve za postupanje s osobnim podacima koje vanjski razvojni inženjeri mogu obrađivati u skladu s GDPR-om.

10.1.5 P24S – Politika sigurnog razvoja: određuje kako interni i vanjski razvoj moraju slijediti prakse sigurnog kodiranja te provjeru biblioteka i razvojnih okvira.

10.1.6 P30S – Politika odgovora na incidente: primjenjuje se kada razvoj vanjskih izvođača dovede do sigurnosnih incidenata ili ranjivosti te usmjerava koordiniranu istragu i otklanjanje posljedica.

10.2 Ove politike moraju se provoditi usporedno kako bi se osiguralo da razvoj vanjskih izvođača ne stvara neupravljani rizik i ne dovodi do kršenja obveza usklađenosti SME-a.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – Organizacije moraju procijeniti i obraditi rizike informacijske sigurnosti povezane s dobavljačima.

11.1.2 Točka 8.1 – Zahtijeva operativno planiranje i kontrolu, uključujući usluge trećih strana kao što je razvoj povjeren vanjskim izvođačima.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – Preporučuje procjenu sposobnosti dobavljača da ispune zahtjeve informacijske sigurnosti.

11.2.2 Kontrola 5.20 – Potiče redovito praćenje i periodični pregled usluga trećih strana.

11.2.3 Kontrole 8.25–8.27 – Opisuju prakse životnog ciklusa sigurnog razvoja primjenjive na razvoj vanjskih izvođača.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Zahtijeva da strategije nabave uključuju mjere informacijske sigurnosti.

11.3.2 SA-9 – Obrađuje vanjski razvoj sustava i rizike opskrbnog lanca.

11.3.3 SA-11 – Definira prakse sigurnog razvoja, uključujući pregled koda i otklanjanje nedostataka.

11.3.4 SA-15 – Potiče uporabu automatiziranih alata za otkrivanje nedostataka i osiguranje softvera.

11.3.5 SR-3 – Nalaže da ugovori s dobavljačima uključuju zahtjeve kibernetičke sigurnosti.

11.4 Opća uredba o zaštiti podataka (GDPR)

11.4.1 Članak 28 – Zahtijeva ugovore s izvršiteljima obrade trećih strana kako bi se osigurale odgovarajuće zaštitne mjere za zaštitu podataka, što se izravno primjenjuje na razvojne inženjere koji obrađuju osobne podatke ili im pristupaju.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(a), (h) – Zahtijeva kontrole sigurnosti opskrbnog lanca i prakse sigurnog razvoja softvera za obuhvaćene pružatelje digitalnih usluga, uključujući SME-ove kada je primjenjivo.

11.6 Uredba EU DORA

11.6.1 Članak 10 – Zahtijeva upravljanje rizicima IKT-a povezanima s trećim stranama, uključujući razvojne ugovore, sigurnosne obveze i kontrole rizika povezane s pružateljima usluga trećih strana.

11.7 COBIT 2019

11.7.1 BAI03 – Upravljanje identifikacijom i izradom rješenja – osigurava da vanjski razvoj ispunjava poslovne zahtjeve i sigurnosna očekivanja.

11.7.2 DSS05 – Upravljanje sigurnosnim uslugama – zahtijeva da vanjske sigurnosne usluge i pružatelji razvojnih usluga djeluju u skladu s primjenjivim sigurnosnim pravilima i nadzorom.