					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P28					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**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8.1	N/A
ISO/IEC 27002:2022	Kontrole 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
GDPR EU	Članci 28, 32	N/A
Direktiva EU NIS2	Članci 21(2)(a), (h), 23	N/A
Uredba EU DORA	Članci 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Svrha

1.1 Ova politika definira obvezne kontrole za povjeravanje razvoja softvera ili sustava vanjskim dobavljačima, ugovornim izvršiteljima ili agencijama te osigurava da su sigurne prakse ugrađene u cjelokupni životni ciklus razvoja.

1.2 Svrha ove politike jest spriječiti sigurnosne ranjivosti, gubitak podataka, izloženost intelektualnog vlasništva (IP) i povrede usklađenosti koje proizlaze iz angažiranja vanjskih razvojnih timova.

1.3 Ova politika uređuje upravljanje dobavljačima, standarde sigurnog kodiranja, upravljanje pristupom, obveze praćenja te postupak izlaska po završetku ugovora radi očuvanja povjerljivosti, cjelovitosti i dostupnosti razvijenog softvera.

2. Opseg

2.1 Ova politika primjenjuje se na sve organizacijske jedinice koje angažiraju vanjske subjekte za razvoj softvera ili sustava, uključujući:

2.1.1 web-aplikacije, mobilne aplikacije, ugrađene sustave, sučelja za programiranje aplikacija, skripte, automatizirane radne tokove ili module platformi

2.1.2 razvoj po mjeri za interne platforme, sustave dostupne klijentima ili komercijalne proizvode

2.1.3 angažmane s razvojnim inženjerima trećih strana, freelancerima, agencijama ili offshore timovima

2.2 Ova politika također uređuje sve vanjske subjekte koji tijekom razvoja pristupaju izvornom kodu, testnim okruženjima ili CI/CD procesima.

2.3 Ovi zahtjevi obvezni su bez obzira na vrstu ugovora, metodologiju razvoja ili geografsku lokaciju vanjski ugovorenog pružatelja usluga.

3. Ciljevi

3.1 Osigurati primjenu praksi sigurnog životnog ciklusa razvoja softvera (SDLC) u svim vanjskim angažmanima, od planiranja do provjere nakon produkcijskog puštanja.

3.2 Osigurati da svi ugovori s vanjskim razvojnim inženjerima uključuju obvezne odredbe o zaštiti podataka, sigurnom kodiranju i zadržavanju intelektualnog vlasništva.

3.3 Definirati zahtjeve za kontrolu pristupa, praćenje i reviziju za razvojne inženjere trećih strana koji rade s internim sustavima.

3.4 Zaštititi organizaciju od rizika opskrbnog lanca, pravnih povreda i reputacijske štete povezane sa softverom koji je razvila treća strana.

3.5 Održavati kontinuiranu usklađenost sa sigurnosnim okvirima, uključujući ISO/IEC 27001, NIST, GDPR, NIS2, DORA i COBIT 2019.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava visokorizične projekte razvoja putem vanjskih pružatelja usluga i potvrđuje iznimke od politike kada su opravdane.

4.1.2 Osigurava da su odluke o vanjskom ugovaranju usklađene sa strateškim ciljevima i apetitom za rizik organizacije.

4.2 Glavni direktor za informacijsku sigurnost (CISO)

4.2.1 Odobrava uvođenje dobavljača sa sigurnosnog stajališta.

4.2.2 Definira zahtjeve za sigurnosne kontrole za vanjske angažmane i pregledava prijave incidenata.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje ili češće u sljedećim okolnostima:

9.1.1 uvođenje novih modela vanjskog razvoja, dobavljača ili nadležnosti

9.1.2 ažuriranja regulatornih okvira kao što su GDPR, NIS2 ili DORA

9.1.3 nakon sigurnosnog incidenta koji uključuje vanjski kod, pristup ili isporučive rezultate

9.1.4 kao dio nalaza interne revizije ili poboljšanja ISMS-a

9.2 Glavni direktor za informacijsku sigurnost (CISO) odgovoran je za pokretanje i koordinaciju pregleda politike u savjetovanju sa:

9.2.1.1 pravnim poslovima i nabavom (radi usklađivanja provedbe ugovornih odredbi)

9.2.1.2 vlasnicima projekata i proizvoda (radi operativne izvedivosti)

9.2.1.3 Timom za informacijsku sigurnost (radi ažuriranja prijetnji i kontrola)

9.2.1.4 izvršnim rukovodstvom (radi konačnog odobrenja)

9.3 Sva ažuriranja politike moraju biti:

9.3.1.1 pod verzijskom kontrolom i pohranjena u određenom repozitoriju dokumenata

9.3.1.2 priopćena dionicima uključenima u aktivnosti razvoja putem vanjskih pružatelja usluga

9.3.1.3 povezana sa svim ažuriranjima povezanih politika ili postupovne dokumentacije

9.4 Svaku verziju politike mora pratiti zapisnik promjena kako bi se osigurala sljedivost izmjena i odobrenja.

10. Povezane politike i poveznice

10.1 Ova politika podupire sljedeće povezane dokumente i oslanja se na njih:

10.1.1 P1 - Politika informacijske sigurnosti: uspostavlja sigurnosna načela na razini organizacije koja se primjenjuju u internom razvoju i razvoju trećih strana.

10.1.2 P5 - Politika upravljanja promjenama: osigurava da se sve promjene povezane s uvođenjem iz vanjskih baza izvornog koda pregledaju i odobre prije provedbe.

10.1.3 P13 - Politika klasifikacije podataka i označavanja: određuje kako se osjetljivi podaci identificiraju prije nego što budu izloženi razvojnim dobavljačima ili repozitorijima.

10.1.4 P18 - Politika kriptografskih kontrola: određuje kako se ključevima, tajnama i osjetljivim vjerodajnicama mora postupati tijekom razvoja i isporuke.

10.1.5 P24 - Politika sigurnog razvoja: definira osnovne zahtjeve za interne i vanjske prakse razvoja softvera.

10.1.6 P30 - Politika odgovora na incidente: uređuje kako se povrede ili sigurnosni problemi povezani s razvojem putem vanjskih pružatelja usluga eskaliraju, istražuju i rješavaju.

10.1.7 P33 - Politika praćenja revizije i usklađenosti: propisuje zahtjeve za pregled aktivnosti razvoja putem vanjskih pružatelja usluga tijekom revizija ili pregleda usklađenosti.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodno priznatim sigurnosnim okvirima i propisima radi osiguranja sigurnog vanjskog ugovaranja razvoja softvera i upravljanja dobavljačima.

11.2 ISO/IEC 27001

11.2.1 Točka 8.1 - Operativno planiranje i kontrola: propisuje procesne kontrole za siguran razvoj i isporuku trećih strana.

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

11.3.1 Dodatak A, kontrola 5.19 - Upravljanje odnosima s dobavljačima: zahtijeva formalne ugovore sa sigurnosnim odredbama i odredbama o usklađenosti.

11.3.2 Dodatak A, kontrola 5.20 - Uključivanje informacijske sigurnosti u ugovore s dobavljačima: osigurava da su kontrole specifične za razvoj ugrađene u ugovore.

11.3.3 Dodatak A, kontrola 5.21 - Upravljanje isporukom usluga dobavljača: uključuje praćenje isporučivih rezultata razvoja trećih strana i povezanih rizika.

11.3.4 Dodatak A, kontrola 8.27 - Vanjski razvoj: propisuje definirane sigurnosne zahtjeve i kontrolu pristupa nad softverom koji se razvija izvan organizacije.

11.3.5 Ove kontrole definiraju strukturirane zahtjeve za odabir, ugovaranje i nadzor vanjskih razvojnih inženjera, uključujući prakse sigurnog razvoja, postupanje s kodom i provjeru učinkovitosti.

11.4 NIST SP 800-53 Rev.

11.4.1 SA-4 - Postupak nabave: zahtijeva da se zahtjevi sigurnog razvoja definiraju u trenutku nabave.

11.4.2 SA-9 - Usluge vanjskih sustava: uređuje kako vanjski razvojni inženjeri sigurno komuniciraju s internim uslugama.

11.4.3 SA-10 - Upravljanje konfiguracijom razvojnih inženjera: usklađeno je s obvezama upravljanja verzijama, pristupa kodu i praćenja promjena za vanjske timove.

11.5 GDPR EU (2016/679)

11.5.1 Članak 28 - Obveze izvršitelja obrade: zahtijeva da ugovori s vanjskim razvojnim inženjerima preciziraju sigurnosne zahtjeve, kontrole i zahtjeve za reviziju pri postupanju s osobnim podacima.

11.5.2 Članak 32 - Sigurnost obrade: propisuje odgovarajuće zaštitne mjere (npr. šifriranje, kontrola pristupa) pri razvoju sustava koji obrađuju osobne podatke.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članci 21(2)(a), (h), 23: zahtijevaju primjenu sigurnih razvojnih praksi u angažmanima trećih strana i digitalnim opskrbnim lancima, uz nadzor i tehničku provjeru.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članci 28(1), (2): zahtijevaju da financijski subjekti upravljaju IKT rizikom trećih strana putem ugovornih kontrola i nadzora sigurnog razvoja, osobito za kritični vanjski razvoj.

11.8 COBIT 2019

11.8.1 APO10 - Upravljanje dobavljačima: uspostavlja strukturirane zahtjeve za procjenu dobavljača, ugovore i praćenje uspješnosti.

11.8.2 BAI03 - Upravljanje izgradnjom rješenja: izravno se povezuje s procesima sigurnog SDLC-a, pregledima koda i provjerom razvoja.

11.8.3 DSS05 - Upravljanje sigurnosnim uslugama: usklađeno je s praćenjem i zaštitom sustava koje razvijaju vanjske strane ili treće strane.