					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P24					Naziv dokumenta: **Politika sigurnog razvoja**							
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**

1. Svrha

1.1 Ova politika definira obvezne sigurnosne zahtjeve za aktivnosti razvoja softvera i sustava u organizaciji, uključujući interne projekte, razvoj koji provode vanjski izvršitelji i integraciju koda trećih strana.

1.2 Cilj je osigurati da je sigurnost ugrađena u cjelokupni životni ciklus razvoja softvera (SDLC) te da se ranjivosti prepoznaju, ublažavaju i sprječavaju prije puštanja u produkcijski rad.

1.3 Ova politika podupire provedbu točke 8.1 norme ISO/IEC 27001:2022 i kontrola 8.25–8.28 Dodatka A standardizacijom upravljanja sigurnim razvojem, praksi pregleda koda i nadzora razvoja koji provode treće strane.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve sljedeće:

2.1.1 Softver, aplikacije, skripte, integracije i alate za automatizaciju razvijene interno ili eksterno

2.1.2 Razvojne timove, vlasnike proizvoda, DevOps inženjere, QA timove, arhitekte, voditelje projekata i ugovorne izvođače

2.1.3 SDLC okruženja, uključujući razvojna, testna, pripremna i pretprodukcijska okruženja

2.1.4 Komponente otvorenog koda i komponente trećih strana integrirane u interne aplikacije

2.1.5 Softver uveden u vlastitom podatkovnom centru, privatnom oblaku, hibridnim okruženjima ili javnom oblaku

2.2 Svi korisnici i svi subjekti koji sudjeluju u razvoju sustava, testiranju ili uvođenju u okviru organizacijskog konteksta podliježu ovoj politici, uključujući pružatelje upravljanih usluga (MSP) i dobavljače platformi.

3. Ciljevi

3.1 Ugraditi sigurnosne kontrole u sve faze razvoja softvera, od dizajna do uvođenja, kako bi smanjenje rizika bilo proaktivno i kontinuirano.

3.2 Spriječiti uvođenje iskoristivih ranjivosti kao što su nedostaci injektiranja, nesigurna autentifikacija i izloženost poznatim slabostima trećih strana.

3.3 Uspostaviti i provoditi prakse sigurnog kodiranja usklađene sa smjernicama OWASP-a, SANS CWE-a i smjernicama specifičnima za pojedini razvojni okvir.

3.4 Osigurati da sav kod prije uvođenja prođe stručni pregled, automatiziranu analizu i sigurnosnu provjeru.

3.5 Upravljati razvojnim rizicima koji proizlaze iz izdvojenih aktivnosti, uključivanja koda trećih strana i ponovne uporabe softvera otvorenog koda.

3.6 Zaštititi razvojna, testna i pripremna okruženja od neovlaštenog pristupa te spriječiti uporabu produkcijskih podataka bez odobrenog maskiranja ili anonimizacije podataka.

3.7 Poticati sigurnosnu osviještenost među razvojnim inženjerima, voditeljima proizvoda i stručnjacima za osiguranje kvalitete putem osposobljavanja temeljenog na ulogama i kontinuiranog informiranja o novim prijetnjama.

4. Uloge i odgovornosti

4.1 Glavni direktor za informacijsku sigurnost (CISO)

4.1.1 Vlasnik je ove politike i osigurava da se zahtjevi sigurnog razvoja provode u cijeloj organizaciji.

4.1.2 Odobrava standarde sigurnog kodiranja i ugovorne aranžmane za razvoj koji provode treće strane.

4.1.3 Odobrava odluke o obradi rizika za neriješene ili odgođene ranjivosti.

4.2 Voditelj sigurnosti aplikacija / DevSecOps menadžer

4.2.1 Izrađuje, održava i promiče smjernice sigurnog kodiranja.

4.2.2 Integrira statičko i dinamičko sigurnosno testiranje u CI/CD procese.

4.2.3 Provodi sigurnosne preglede koda i određuje obvezne korektivne mjere.

[... 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 pregledavati najmanje jednom godišnje ili češće kao odgovor na:

9.1.1 Značajne izmjene razvojnih metodologija ili DevOps alata

9.1.2 Značajne sigurnosne incidente koji proizlaze iz ranjivosti aplikacija

9.1.3 Promjene regulatornih zahtjeva povezanih sa sigurnim softverom (npr. GDPR, DORA)

9.1.4 Nove industrijske standarde ili obavijesti o prijetnjama i ranjivostima (npr. OWASP Top 10, SLSA, MITRE CWE)

9.2 Pregled politike vodi Voditelj sigurnosti aplikacija u koordinaciji s Glavnim direktorom za informacijsku sigurnost (CISO), softverskim arhitektima, vodstvom QA-a i pravnim savjetnikom (za implikacije koda trećih strana).

9.3 Sve izmjene moraju se evidentirati u registru kontrole dokumenata ISMS-a, staviti pod upravljanje verzijama i priopćiti pogođenim timovima putem napomena uz izdanje ili obvezne obuke.

9.4 Prethodne verzije moraju se čuvati u arhivskom repozitoriju radi pravne sljedivosti i revizijskog traga.

10. Povezane politike i upućivanja

10.1 P1 – Politika informacijske sigurnosti. Utvrđuje strateški mandat za ugradnju sigurnosti u sve informacijske sustave, pri čemu je siguran razvoj temeljna operativna kontrola.

10.2 P4 – Politika kontrole pristupa. Definira kontrolne mjere za ograničavanje pristupa razvojnim okruženjima, repozitorijima, alatima za izgradnju i CI/CD procesima.

10.3 P5 – Politika upravljanja promjenama. Osigurava da promjene koda, izdanja i uvođenja podliježu odgovarajućem odobrenju, planiranju povrata i provjeri nakon uvođenja.

10.4 P12 – Politika upravljanja imovinom. Podupire evidentiranje razvojnih okruženja, izvornih repozitorija i sustava za izgradnju kao upravljane imovine koja podliježe klasifikaciji i zaštiti.

10.5 P22 – Politika bilježenja i praćenja. Primjenjuje se na razvojne procese i osigurava da se postupci izgradnje, promicanje koda i događaji uvođenja bilježe, prate i analiziraju radi otkrivanja sigurnosnih anomalija.

10.6 P30 – Politika odgovora na incidente. Pruža okvir za analizu i odgovor na sigurnosne nedostatke otkrivene nakon uvođenja ili tijekom sigurnosnog testiranja aplikacija.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – Operativno planiranje i kontrola: zahtijeva integraciju procesa i kontrola sigurnog razvoja u operativne aktivnosti.

11.2 ISO/IEC 27002:2022 – Kontrole 8.25–8.28

11.2.1 Kontrola 8.25 Dodatka A – Životni ciklus sigurnog razvoja: zahtijeva formalno uključivanje sigurnosti u dizajn i razvoj softvera.

11.2.2 Kontrola 8.26 Dodatka A – Zahtjevi sigurnosti aplikacija: zahtijeva definiranje sigurnog kodiranja i kriterija sigurnosnog prihvaćanja.

11.2.3 Kontrola 8.27 Dodatka A – Sigurna arhitektura sustava i inženjerska načela: zahtijeva primjenu načela sigurnog dizajna i ublažavanje poznatih slabosti.

11.2.4 Kontrola 8.28 Dodatka A – Sigurno kodiranje: zahtijeva uspostavu i primjenu praksi sigurnog kodiranja.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 do SA-15: uspostavlja strukturirane prakse razvoja sigurnosti aplikacija, uključujući zahtjeve za dizajn, cjelovitost koda i testiranje.

11.3.2 SI-10 – Provjera ulaznih informacija: odnosi se na zaštitne mjere sigurnog kodiranja.

11.3.3 SR-3 – Zaštita opskrbnog lanca: zahtijeva provjeru softvera trećih strana, komponenti i pružatelja razvojnih usluga.

11.4 GDPR EU (2016/679)

11.4.1 Članak 25 – zaštita podataka u fazi projektiranja i zaštita podataka prema zadanim postavkama: zahtijeva ugradnju sigurnosti i privatnosti u razvoj sustava.

11.4.2 Članak 32 – Sigurnost obrade: podupire tehničke mjere kao što su provjera ulaznih podataka, kontrole pristupa i sigurno uvođenje.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(e–f): zahtijeva prakse razvoja softvera koje uključuju upravljanje ranjivostima, sigurnost koda i prijavljivanje incidenata.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – upravljanje IKT rizicima: zahtijeva prakse sigurnog razvoja za financijske subjekte, uključujući kontrole kvalitete softvera i otklanjanje nedostataka.

11.6.2 Članak 10 – kontinuitet poslovanja i testiranje: potiče strogo testiranje i validaciju IKT sustava, uključujući aplikacije.

11.7 COBIT 2019

11.7.1 BAI03 – Upravljanje identifikacijom i izgradnjom rješenja: uređuje dizajn, razvoj i integraciju sigurnosti u nova rješenja.

11.7.2 BAI07 – Upravljanje prihvaćanjem promjena i prijelazom: osigurava sigurno uvođenje i ocjenu nakon uvođenja.

11.7.3 DSS05 – Upravljanje sigurnosnim uslugama: primjenjuje sigurnosnu provjeru na isporuku softvera i usluga.