					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P24S					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**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Relevantne sigurnosne kontrole za operativne prakse, uključujući siguran razvoj
ISO/IEC 27002:2022	Kontrole 8.25–8.27	Obuhvaća životni ciklus sigurnog razvoja sustava, testiranje i sigurnosne odgovornosti vanjskih razvojnih inženjera
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Obuhvaća sigurni SDLC, kontrolu pristupa i upravljanje ranjivostima u razvoju
GDPR EU	Članak 25	Zahtijeva zaštitu podataka u fazi projektiranja i zaštitu privatnosti prema zadanim postavkama u razvoju softvera
Direktiva EU NIS2	Članak 21(2)(a), (e), (h)	Zahtijeva politike sigurnog razvoja, nadzor nad korištenjem otvorenog koda i dokumentiranje mjera ublažavanja
Uredba EU DORA	Članci 6(7), 9(1)(c), 10(2)(c)	Sigurnost životnog ciklusa za kritične IKT sustave u financijskom sektoru
COBIT 2019	BAI	Okvir za strukturirano, sljedivo i otporno upravljanje sigurnim razvojem

1. Svrha

1.1 Ova politika osigurava da se sav softver, skripte i alati temeljeni na webu koje organizacija ili njezini vanjski partneri razvijaju ili mijenjaju razvijaju na siguran način, uz smanjenje rizika od ranjivosti, neovlaštenog pristupa podacima i operativnih poremećaja.

1.2 Ova politika utvrđuje obvezna pravila sigurnog razvoja i sigurnog kodiranja kojih se moraju pridržavati svi interni razvojni inženjeri, ugovorni izvođači i dobavljači, neovisno o veličini ili složenosti projekta.

1.3 Ova politika namijenjena je zaštiti podataka klijenata, sprječavanju povreda i osiguravanju da softver koji je organizacija razvila ili prilagodila, ili koji je razvijen ili prilagođen za organizaciju, može zadovoljiti zahtjeve sigurnosnih revizija, pravne zahtjeve (npr. GDPR, NIS2, DORA) i podržati certifikaciju prema normi ISO/IEC 27001.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve osobe i subjekte uključene u razvoj, prilagodbu, uvođenje ili upravljanje sljedećim rješenjima u ime organizacije:

2.1.1 internetske stranice, aplikacije ili alati za automatizaciju

2.1.2 interno razvijene skripte ili softver

2.1.3 kod koji su razvili vanjski razvojni inženjeri ili freelanceri

2.1.4 dodaci, biblioteke i softverske komponente integrirane u produkcijske sustave

2.2 Ova politika obuhvaća sva okruženja koja se koriste u razvojnim aktivnostima, uključujući:

2.2.1 razvojna i testna okruženja

2.2.2 pripremna i pretprodukcijska okruženja

2.2.3 produkcijske sustave koji se koriste za izvršavanje koda razvijenog po mjeri

2.3 Ova politika uređuje i postupanje s podacima tijekom razvoja i uvođenja, osobito svaku uporabu produkcijskih podataka u neprodukcijskom okruženju.

3. Ciljevi

3.1 Spriječiti unošenje sigurnosnih slabosti ili ranjivosti u softver razvijen po mjeri ili softver koji su razvile treće strane.

3.2 Osigurati da su prakse sigurnog kodiranja i sprječavanje ranjivosti ugrađeni u svaku fazu životnog ciklusa razvoja softvera.

3.3 Smanjiti rizike povezane s uporabom komponenti otvorenog koda ili komponenti trećih strana propisivanjem odgovarajuće provjere i praćenja.

3.4 Zahtijevati formalni pregled koda i sigurnosno testiranje aplikacija prije izdanja.

3.5 Kontrolirati pristup razvojnim okruženjima i osigurati njihovo odvajanje od aktivnih produkcijskih sustava.

3.6 Ispuniti obvezne zahtjeve međunarodnih normi i propisa (npr. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Uloge i odgovornosti

4.1 glavni rukovoditelj (GM)

4.1.1 Odobrava ovu politiku i odgovoran je za njezinu provedbu.

4.1.2 Osigurava da je sav razvoj softvera, interni ili vanjski, usklađen s ovom politikom.

4.1.3 Pregledava i odobrava ugovore o razvoju ili pružanju usluga koji uključuju odredbe o sigurnom razvoju.

4.1.4 Provjerava usklađenost dobavljača redovitim provjerama ili zahtijevanjem sigurnosnih dokaza.

4.2 interni razvojni inženjer ili vlasnik aplikacije

4.2.1 Pridržava se praksi sigurnog kodiranja i sigurnog uvođenja.

4.2.2 Primjenjuje kontrolni popis sigurnog razvoja na svaki projekt.

4.2.3 Provjerava sigurnost svih korištenih komponenti otvorenog koda ili komponenti trećih strana.

4.2.4 Svaku otkrivenu ranjivost odmah prijavljuje GM-u.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku mora pregledati glavni rukovoditelj najmanje jednom godišnje kako bi:

9.1.1 provjerio trajnu usklađenost s ISO/IEC 27001, GDPR-om, NIS2 i Uredbom EU DORA

9.1.2 uzeo u obzir nove prijetnje ili promjene najboljih praksi sigurnog razvoja

9.1.3 osigurao usklađenost s novim alatima, platformama ili odnosima s dobavljačima

9.2 Izvanredni pregledi moraju se provesti u slučaju:

9.2.1 svakog prijavljenog sigurnosnog incidenta povezanog sa softverom

9.2.2 uvođenja novog razvojnog okvira ili platforme za hosting

9.2.3 promjene partnera za razvoj trećih strana

9.2.4 regulatornih ažuriranja koja utječu na obveze povezane sa softverom ili sigurnošću

9.3 Sve promjene ove politike moraju biti:

9.3.1 dokumentirane s datumom, sažetkom promjene i odobrenjem GM-a

9.3.2 jasno priopćene svom internom i vanjskom razvojnom osoblju

9.3.3 pohranjene kao dio upravljanja verzijama politike i povijesti promjena organizacije

9.4 Ažurirane verzije moraju biti lako dostupne putem internih platformi, tiskane dokumentacije ili usluga u oblaku dostupnih dobavljačima.

10. Povezane politike i poveznice

10.1 Ova politika podržava i ovisi o uspješnoj provedbi nekoliko drugih SME politika:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: uspostavlja odgovornost za dodjelu i provjeru kontrola sigurnosti razvoja kroz projekte i dobavljače.

10.1.2 P4S – Politika kontrole pristupa: pruža osnovna pravila za ograničavanje pristupa razvojnim okruženjima i repozitorijima koda, uključujući razdvajanje dužnosti (SoD).

10.1.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da interni razvojni inženjeri i ugovorni izvođači razumiju prakse sigurnog kodiranja i povezane sigurnosne odgovornosti.

10.1.4 P17S – Politika zaštite podataka i privatnosti: pojašnjava kako se s osobnim podacima mora postupati tijekom razvoja, testiranja i evidentiranja kako bi se održala usklađenost s GDPR-om.

10.1.5 P30S – Politika odgovora na incidente: definira kako se sigurnosni incidenti povezani s razvojem moraju prijaviti, procijeniti i otkloniti, uključujući izloženosti povezane s kodom.

10.2 Svaka od ovih politika djeluje zajedno kako bi siguran razvoj bio provediv i dokaziv, čak i u maloj ili netehničkoj organizaciji.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – zahtijeva provedbu operativnih kontrola, uključujući siguran razvoj, usklađenih s poslovnim ciljevima i profilom rizika.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – preporučuje integriranje sigurnosti kroz cijeli životni ciklus softvera, uključujući kontrolu izvornog koda, upravljanje verzijama i pristup razvojnih inženjera.

11.2.2 Kontrola 8.26 – određuje metode testiranja aplikacija i provjere sigurnosne funkcionalnosti prije puštanja u produkcijski rad.

11.2.3 Kontrola 8.27 – zahtijeva da se vanjski razvojni inženjeri pridržavaju istih razvojnih standarda te da njihove sigurnosne odgovornosti budu jasno definirane.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 do SA-15 – definiraju procese sigurnog razvoja, uključujući kontrolu pristupa razvojnih inženjera, testiranje, modeliranje prijetnji i dokumentaciju.

11.3.2 SI-10 – zahtijeva da razvojni inženjeri identificiraju i ublaže uobičajene sigurnosne slabosti softvera te koriste automatizirane alate kada je to primjenjivo.

11.4 GDPR EU (2016/679)

11.4.1 Članak 25 – „zaštita podataka u fazi projektiranja i zaštita privatnosti prema zadanim postavkama” nalaže integriranje zaštite sigurnosti i privatnosti tijekom projektiranja i razvoja softvera, osobito kada se obrađuju osobni podaci.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(a), (e) i (h) – zahtijeva politike sigurnog razvoja, nadzor nad korištenjem otvorenog koda i dokumentirano ublažavanje rizika povezanih s aplikacijama u ključnim i važnim subjektima.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članci 6(7), 9(1)(c) i 10(2)(c) – nameću obveze sigurnosti životnog ciklusa razvoja subjektima financijskog sektora, uključujući SME, osobito za kritične IKT sustave.

11.7 COBIT 2019

11.7.1 BAI03 – „Upravljanje identifikacijom i izradom rješenja" podržava provedbu strukturiranih razvojnih kontrola koje naglašavaju sigurnost, sljedivost i otpornost, prilagođenih ograničenjima SME okruženja.