					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P24S					Naslov dokumenta: **Politika varnega razvoja**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Pravno obvestilo (avtorske pravice in omejitve uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.

Nepooblaščena uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.

Za licenciranje se obrnite na: info@clarysec.com

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Ustrezne varnostne kontrole za operativne prakse, vključno z varnim razvojem
ISO/IEC 27002:2022	Kontrole 8.25–8.27	Obravnava življenjski cikel varnega razvoja, testiranje in varnostne odgovornosti zunanjih razvijalcev
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Obravnava varen življenjski cikel razvoja programske opreme, nadzor dostopa in obravnavo ranljivosti v razvoju
Uredba EU GDPR	Člen 25	Zahteva varstvo podatkov že pri načrtovanju in privzeto varstvo zasebnosti pri razvoju programske opreme
Direktiva EU NIS2	Člen 21(2)(a), (e), (h)	Zahteva politike varnega razvoja, nadzor nad uporabo odprtokodnih rešitev in dokumentiranje ukrepov za zmanjšanje tveganj
Uredba EU DORA	Členi 6(7), 9(1)(c), 10(2)(c)	Varnost življenjskega cikla za kritične sisteme IKT v finančnem sektorju
COBIT 2019	BAI	Okvir za strukturirano, sledljivo in odporno upravljanje varnega razvoja

1. Namen

1.1 Ta politika zagotavlja, da so vsa programska oprema, skripti in spletna orodja, ki jih organizacija ali njeni zunanji partnerji ustvarijo ali spremenijo, razviti na varen način, s čimer se zmanjša tveganje ranljivosti, nepooblaščenega dostopa do podatkov ali operativnih motenj.

1.2 Določa obvezna pravila varnega razvoja in prakse varnega kodiranja, ki jih morajo upoštevati vsi interni razvijalci, pogodbeni izvajalci in dobavitelji, ne glede na velikost ali kompleksnost projekta.

1.3 Ta politika je namenjena zaščiti podatkov strank, preprečevanju kršitev in zagotavljanju, da programska oprema, ki jo organizacija ali zanjo razvije ali prilagodi, uspešno prestane varnostne presoje, izpolnjuje pravne zahteve (npr. GDPR, NIS2, DORA) in podpira certificiranje po ISO/IEC 27001.

2. Področje uporabe

2.1 Ta politika velja za vse posameznike in subjekte, vključene v razvoj, prilagajanje, uvajanje ali upravljanje naslednjega v imenu organizacije:

2.1.1 spletnih mest, aplikacij ali orodij za avtomatizacijo,

2.1.2 interno razvitih skriptov ali programske opreme,

2.1.3 kode, ki jo ustvarijo zunanji razvijalci ali samostojni izvajalci,

2.1.4 vtičnikov, knjižnic in programskih komponent, integriranih v produkcijske sisteme.

2.2 Zajema vsa okolja, ki se uporabljajo pri razvojnih dejavnostih, vključno z:

2.2.1 razvojnimi in testnimi okolji,

2.2.2 pripravljalnimi in predprodukcijskimi okolji,

2.2.3 produkcijskimi sistemi, ki se uporabljajo za izvajanje kode po meri.

2.3 Politika ureja tudi ravnanje s podatki med razvojem in uvajanjem, zlasti uporabo produkcijskih podatkov v neprodukcijskih sistemih.

3. Cilji

3.1 Preprečiti vnos varnostnih pomanjkljivosti ali ranljivosti v programsko opremo po meri ali programsko opremo, ki jo razvijejo tretje osebe.

3.2 Zagotoviti, da so prakse varnega kodiranja in preprečevanje ranljivosti vključeni v vsako fazo življenjskega cikla razvoja programske opreme.

3.3 Zmanjšati tveganja, povezana z uporabo odprtokodnih komponent ali komponent tretjih oseb, z zahtevo po ustreznem preverjanju in sledljivosti.

3.4 Zahtevati formalni pregled izvorne kode in varnostno testiranje aplikacij pred izdajo.

3.5 Nadzorovati dostop do razvojnih okolij in zagotoviti njihovo ločitev od produkcijskih sistemov.

3.6 Izpolniti obvezne zahteve mednarodnih standardov in predpisov (npr. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Odobri to politiko in je njen lastnik.

4.1.2 Zagotavlja, da je ves razvoj programske opreme, interni ali zunanji, skladen s to politiko.

4.1.3 Pregleduje in podpisuje razvojne ali storitvene pogodbe, ki vključujejo klavzule o varnem razvoju.

4.1.4 Preverja skladnost dobaviteljev z rednimi pregledi ali z zahtevo po predložitvi revizijskih dokazil.

4.2 Interni razvijalec ali lastnik aplikacije

4.2.1 Upošteva prakse varnega kodiranja in postopke uvajanja.

4.2.2 Za vsak projekt uporabi kontrolni seznam varnega razvoja.

4.2.3 Preveri varnost vseh uporabljenih odprtokodnih komponent ali komponent tretjih oseb.

4.2.4 O vseh odkritih ranljivostih nemudoma poroča GM.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko mora Generalni direktor pregledati najmanj enkrat letno, da:

9.1.1 preveri nadaljnjo skladnost z ISO/IEC 27001, GDPR, NIS2 in DORA,

9.1.2 upošteva posodobljene grožnje ali spremembe dobrih praks varnega razvoja,

9.1.3 zagotovi združljivost z novimi orodji, platformami ali odnosi z dobavitelji.

9.2 Vmesni pregledi se morajo sprožiti ob:

9.2.1 vsakem prijavljenem varnostnem incidentu programske opreme,

9.2.2 uvedbi novega razvojnega ogrodja ali platforme gostovanja,

9.2.3 spremembi zunanjih razvojnih partnerjev,

9.2.4 regulativnih posodobitvah, ki vplivajo na programsko opremo ali varnostne obveznosti.

9.3 Vse spremembe te politike morajo biti:

9.3.1 dokumentirane z datumom, povzetkom spremembe in odobritvijo GM,

9.3.2 jasno sporočene vsem internim in zunanjim članom razvojnega osebja,

9.3.3 shranjene kot del nadzora različic politike in evidence sprememb organizacije.

9.4 Posodobljene različice morajo biti enostavno dostopne prek internih platform, tiskane dokumentacije ali storitev v oblaku, dostopnih dobaviteljem.

10. Povezane politike in povezave

10.1 Ta politika podpira in je odvisna od uspešnega izvajanja več drugih politik SME:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornost za dodeljevanje in preverjanje kontrol varnega razvoja v projektih in pri dobaviteljih.

10.1.2 P4S – Politika nadzora dostopa: določa osnovna pravila za omejevanje dostopa do razvojnih okolij in repozitorijev kode, vključno z ločevanjem dolžnosti (SoD).

10.1.3 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da interni razvijalci in pogodbeni izvajalci razumejo prakse varnega kodiranja in povezane varnostne odgovornosti.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: pojasnjuje, kako je treba z osebnimi podatki ravnati med razvojem, testiranjem in beleženjem dnevnikov, da se zagotovi skladnost z GDPR.

10.1.5 P30S – Politika odzivanja na incidente: določa, kako je treba poročati o varnostnih incidentih, povezanih z razvojem, jih oceniti in odpraviti, vključno z razkritji, povezanimi s kodo.

10.2 Vse te politike skupaj zagotavljajo, da je varen razvoj dosegljiv in preverljiv tudi v majhni ali netehnični organizaciji.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Zahteva uvedbo operativnih kontrol, vključno z varnim razvojem, ki so usklajene s poslovnimi cilji in profilom tveganja.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.25 – Priporoča vključevanje varnosti skozi celoten življenjski cikel programske opreme, vključno z nadzorom izvorne kode, različicami in dostopom razvijalcev.

11.2.2 Kontrola 8.26 – Določa metode za testiranje aplikacij in preverjanje varnostne funkcionalnosti pred prehodom v produkcijo.

11.2.3 Kontrola 8.27 – Zahteva, da zunanji razvijalci upoštevajo enake razvojne standarde in da so njihove varnostne odgovornosti jasno opredeljene.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 do SA-15 – Določajo procese varnega razvoja, vključno z nadzorom dostopa razvijalcev, testiranjem, modeliranjem groženj in dokumentacijo.

11.3.2 SI-10 – Zahteva, da razvijalci prepoznajo in zmanjšujejo pogoste slabosti programske opreme ter po potrebi uporabljajo avtomatizirana orodja.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 25 – »Varstvo podatkov že pri načrtovanju in privzeto varstvo zasebnosti« zahteva vključitev zaščite varnosti in zasebnosti v zasnovo in razvoj programske opreme, zlasti kadar se obdelujejo osebni podatki.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a), (e) in (h) – Zahteva politike varnega razvoja, nadzor nad uporabo odprtokodnih rešitev in dokumentirano zmanjševanje tveganj, povezanih z aplikacijami, pri bistvenih in pomembnih subjektih.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Členi 6(7), 9(1)(c) in 10(2)(c) – Nalagajo obveznosti glede varnosti življenjskega cikla razvoja za subjekte finančnega sektorja, vključno z MSP, zlasti za kritične sisteme IKT.

11.7 COBIT 2019

11.7.1 BAI03 – »Upravljanje identifikacije in izgradnje rešitev« podpira uvedbo strukturiranih razvojnih kontrol, ki poudarjajo varnost, sledljivost in odpornost, prilagojeno omejitvam SME.