					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P24					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

1. Namen

1.1 Ta politika določa obvezne varnostne zahteve za razvoj programske opreme in sistemov v organizaciji, vključno z internimi projekti, zunanjim razvojem in integracijo kode tretjih oseb.

1.2 Cilj politike je zagotoviti, da je varnost vključena v celoten življenjski cikel razvoja programske opreme (SDLC) ter da so ranljivosti prepoznane, obravnavane in preprečene pred uvedbo v produkcijo.

1.3 Ta politika podpira izvajanje klavzule 8.1 standarda ISO/IEC 27001:2022 in kontrol Priloge A 8.25–8.27 s standardizacijo upravljanja varnega razvoja, praks pregledovanja kode in nadzora nad razvojem tretjih oseb.

2. Področje uporabe

2.1 Ta politika velja za vse:

2.1.1 interno ali eksterno razvite programske rešitve, aplikacije, skripte, integracije in orodja za avtomatizacijo

2.1.2 razvojne ekipe, lastnike produktov, inženirje DevOps, ekipe za zagotavljanje kakovosti, arhitekte, vodje projektov in pogodbene izvajalce

2.1.3 okolja SDLC, vključno z razvojnimi, testnimi, pripravljalnimi in predprodukcijskimi sistemi

2.1.4 odprtokodne komponente in komponente tretjih oseb, vključene v interne aplikacije

2.1.5 programsko opremo, uvedeno v lastnem okolju, zasebnem oblaku, hibridnem oblaku ali javnem oblaku

2.2 Vsi uporabniki in subjekti, ki sodelujejo pri razvoju, testiranju ali uvajanju sistemov v organizacijskem okolju, so zavezani tej politiki, vključno s ponudniki upravljanih storitev (MSP) in ponudniki platform.

3. Cilji

3.1 Vključiti varnostne kontrole v vse faze razvoja programske opreme, od načrtovanja do uvajanja, ter zagotoviti, da se tveganja zmanjšujejo proaktivno in neprekinjeno.

3.2 Preprečiti vnos izkoristljivih ranljivosti, kot so vrivanie kode, neustrezna avtentikacija in izpostavljenost znanim slabostim komponent tretjih oseb.

3.3 Določiti in uveljaviti prakse varnega razvoja kode, usklajene z OWASP, SANS CWE in smernicami, specifičnimi za posamezne okvire.

3.4 Zagotoviti, da je vsa koda pred uvedbo predmet medsebojnega strokovnega pregleda, avtomatizirane analize in varnostnega preverjanja.

3.5 Upravljati razvojna tveganja, ki izhajajo iz zunanjega izvajanja, vključevanja kode tretjih oseb in ponovne uporabe odprtokodne programske opreme.

3.6 Zaščititi razvojna, testna in pripravljalna okolja pred nepooblaščenim dostopom ter preprečiti uporabo produkcijskih podatkov brez odobrenega maskiranja ali anonimizacije podatkov.

3.7 Spodbujati varnostno ozaveščenost med razvijalci, vodji produktov in strokovnjaki za zagotavljanje kakovosti z usposabljanjem po vlogah in stalnim obveščanjem o nastajajočih grožnjah.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja, da se zahteve varnega razvoja uveljavljajo na ravni celotne organizacije.

4.1.2 Odobrava standarde varnega razvoja kode in pogodbena določila za razvoj tretjih oseb.

4.1.3 Potrjuje odločitve o obravnavi tveganj za neodpravljene ali odložene ranljivosti.

4.2 Vodja varnosti aplikacij / vodja DevSecOps

4.2.1 Pripravlja, vzdržuje in promovira smernice za varni razvoj kode.

4.2.2 Vključuje statično in dinamično varnostno testiranje v cevovode CI/CD.

4.2.3 Izvaja varnostne preglede kode in določa obvezne ukrepe za odpravo pomanjkljivosti.

[... 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 je treba pregledati letno ali pogosteje kot odziv na:

9.1.1 večje spremembe razvojnih metodologij ali orodij DevOps

9.1.2 pomembne varnostne incidente, ki izhajajo iz ranljivosti aplikacij

9.1.3 spremembe regulativnih zahtev, povezanih z varno programsko opremo (npr. GDPR, DORA)

9.1.4 nove panožne standarde ali obveščevalne podatke o grožnjah (npr. OWASP Top 10, SLSA, MITRE CWE)

9.2 Pregled politike vodi vodja varnosti aplikacij v sodelovanju z vodjo informacijske varnosti (CISO), arhitekti programske opreme, vodstvom zagotavljanja kakovosti in pravno službo (zaradi posledic glede kode tretjih oseb).

9.3 Vse spremembe morajo biti zabeležene v registru dokumentov ISMS, upravljane po različicah in sporočene zadevnim ekipam prek opomb ob izdaji ali obveznega usposabljanja.

9.4 Starejše različice je treba hraniti v arhivskem repozitoriju zaradi pravne sledljivosti in revizijske sledljivosti.

10. Povezane politike in povezave

10.1 P1 – Politika informacijske varnosti. Določa strateški okvir za vključevanje varnosti v vse informacijske sisteme, pri čemer je varni razvoj temeljna operativna kontrola.

10.2 P4 – Politika nadzora dostopa. Določa kontrolne ukrepe za omejevanje dostopa do razvojnih okolij, repozitorijev, orodij za gradnjo in cevovodov CI/CD.

10.3 P5 – Politika upravljanja sprememb. Zagotavlja, da so spremembe kode, izdaje in uvedbe predmet ustrezne odobritve, načrtov povrnitve in preverjanja po uvedbi.

10.4 P12 – Politika upravljanja sredstev. Podpira popis razvojnih okolij, izvornih repozitorijev in sistemov za gradnjo kot upravljanih sredstev, ki so predmet razvrščanja in zaščite.

10.5 P22 – Politika beleženja in spremljanja. Velja za razvojne cevovode ter zagotavlja, da so procesi gradnje, prenosi kode in dogodki uvajanja beleženi, spremljani in analizirani glede varnostnih anomalij.

10.6 P30 – Politika odzivanja na incidente. Določa okvir za analizo in odzivanje na varnostne pomanjkljivosti, odkrite po uvedbi ali med varnostnim testiranjem aplikacij.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – Operativno načrtovanje in kontrola: zahteva vključitev procesov in kontrol varnega razvoja v operativne postopke.

11.2 ISO/IEC 27002:2022 – Kontrole 8.25–8.27

11.2.1 Kontrola Priloge A 8.25 – življenjski cikel varnega razvoja: zahteva formalno vključitev varnosti v zasnovo in razvoj programske opreme.

11.2.2 Kontrola Priloge A 8.26 – varnostne zahteve za aplikacije: zahteva opredelitev zahtev varnega razvoja kode in meril varnostne sprejemljivosti.

11.2.3 Kontrola Priloge A 8.27 – načela varne arhitekture in inženiringa sistemov: zahteva uporabo načel varnostne zasnove in ublažitev znanih slabosti.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 do SA-15: določajo strukturirane prakse razvoja varnosti aplikacij, vključno z zahtevami glede zasnove, integritete kode in testiranja.

11.3.2 SI-10 – preverjanje vhodnih podatkov: obravnava zaščitne ukrepe varnega razvoja kode.

11.3.3 SR-3 – zaščita dobavne verige: zahteva preverjanje programske opreme tretjih oseb, komponent in razvojnih ponudnikov.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 25 – varstvo podatkov pri načrtovanju in privzeto: zahteva vključitev varnosti in zasebnosti v razvoj sistemov.

11.4.2 Člen 32 – varnost obdelave: podpira tehnične ukrepe, kot so preverjanje vhodnih podatkov, kontrole dostopa in varna uvedba.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(e–f): zahteva prakse razvoja programske opreme, ki vključujejo upravljanje ranljivosti, varnost kode in poročanje o incidentih.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – upravljanje tveganj IKT: zahteva prakse varnega razvoja za finančne subjekte, vključno s kontrolami kakovosti programske opreme in odpravo napak.

11.6.2 Člen 10 – neprekinjeno poslovanje in testiranje: spodbuja strogo testiranje in preverjanje sistemov IKT, vključno z aplikacijami.

11.7 COBIT 2019

11.7.1 BAI03 – upravljanje identifikacije rešitev in gradnje: ureja zasnovo, razvoj in vključitev varnosti v nove rešitve.

11.7.2 BAI07 – upravljanje sprejema sprememb in prehoda: zagotavlja varno uvedbo in ocenjevanje po uvedbi.

11.7.3 DSS05 – upravljanje varnostnih storitev: uporablja varnostno preverjanje za programsko opremo in izvajanje storitev.