					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P25					Naslov dokumenta: **Politika zahtev informacijske varnosti aplikacij**							
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	—
ISO/IEC 27002:2022	Kontrole 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
Uredba EU GDPR	Člena 25, 32	—
Direktiva EU NIS2	Člena 21(2)(f), 23	—
Uredba EU DORA	Člena 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Namen

1.1 Ta politika določa obvezne zahteve informacijske varnosti na ravni aplikacij za programsko opremo, ki jo organizacija razvija, nabavlja, integrira ali uvaja. Zagotavlja, da so vse aplikacije zasnovane, implementirane in vzdrževane v skladu z načeli varnega razvoja, regulatornimi obveznostmi in apetitom organizacije po tveganju.

1.2 Ta politika zahteva vključitev varnosti v celoten življenjski cikel aplikacije, vključno z avtentikacijo uporabnikov, obravnavo podatkov, zaščito vmesnikov in varno interakcijo z vmesniki za aplikacijsko programiranje ali storitvami.

1.3 Organizacija s sprejetjem te politike preprečuje vnos ranljivosti v programsko opremo, varuje občutljive podatke ter zagotavlja sledljivost in odpornost proti izkoriščanju in zlorabam.

2. Področje uporabe

2.1 Ta politika se uporablja za vse:

2.1.1 interno razvite ali zunanje pridobljene aplikacije, vključno s storitvami SaaS in rešitvami po meri,

2.1.2 aplikacije, ki podpirajo kritične poslovne procese, dostop strank ali obdelavo reguliranih podatkov,

2.1.3 razvojne ekipe, ekipe DevOps, ekipe za zagotavljanje kakovosti (QA), produktne ekipe in ekipe informacijske varnosti,

2.1.4 zunanje razvijalce, dobavitelje programske opreme in integracijske partnerje z dostopom do aplikacij organizacije ali vmesnikov za aplikacijsko programiranje.

2.2 Uporablja se v vseh okoljih: razvoj, testiranje, predprodukcija, produkcija in okolje za obnovitev po nesreči, ne glede na to, ali so sistemi gostovani v lastnih prostorih, zasebnih podatkovnih centrih ali javnem oblaku.

3. Cilji

3.1 Določiti osnovne funkcionalne in nefunkcionalne varnostne zahteve, ki jih morajo izpolnjevati vse aplikacije ne glede na način razvoja ali tehnološki sklad.

3.2 Zagotoviti vključitev zaščitnih ukrepov na ravni aplikacij, vključno s preverjanjem vhodov, kodiranjem izhodov, obravnavo napak in varnostjo sej.

3.3 Zahtevati varno implementacijo mehanizmov avtentikacije, avtorizacije in nadzora dostopa, usklajenih s politikami organizacije na področju upravljanja identitet in dostopov.

3.4 Določiti varno interakcijo z vmesniki za aplikacijsko programiranje, spletnimi vmesniki in komponentami tretjih oseb z uporabo odobrenih protokolov in varnostnih kontrol.

3.5 Omogočiti zgodnje zaznavanje in zmanjševanje ranljivosti s statično in dinamično analizo, pregledom izvorne kode in modeliranjem groženj.

3.6 Varovati občutljive podatke v skladu z regulatornimi zahtevami z uveljavljanjem šifriranja, klasifikacije in pravil hrambe podatkov.

3.7 Zagotoviti stalno preverjanje profila tveganja na področju varnosti aplikacij po uvedbi s testiranjem, spremljanjem in revizijsko pripravljenostjo.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost s strategijo informacijske varnosti in profilom tveganja organizacije.

4.1.2 Odobri zahteve informacijske varnosti aplikacij in zahteva obvezne kontrole v razvojnih funkcijah in pri nabavi.

4.2 Vodja varnosti aplikacij / vodja DevSecOps

4.2.1 Določa osnovni nabor varnostnih kontrol in metodologij testiranja za komponente aplikacij.

4.2.2 Nadzira varno integracijo orodij, kot so SAST, DAST, IAST in SCA, v proces dobave programske opreme.

4.2.3 Vzdržuje kontrolni seznam zahtev informacijske varnosti aplikacij in merila preverjanja.

[... 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 Ta politika se mora pregledati letno ali pogosteje kot odziv na:

9.1.1 obvestila o kritičnih ranljivostih, ki vplivajo na pogosto uporabljena ogrodja ali odvisnosti,

9.1.2 posodobitve regulatornih obveznosti na področju varnosti aplikacij (npr. NIS2, DORA),

9.1.3 večje spremembe praks razvoja programske opreme, orodij ali arhitekture oblaka v organizaciji,

9.1.4 ugotovitve notranjih revizij ali zunanjih penetracijskih testiranj.

9.2 Pregled vodi vodja varnosti aplikacij v koordinaciji z vodjo informacijske varnosti, inženiringom DevOps, pravno službo, nabavo in vodji QA.

9.3 Vse spremembe morajo biti verzionirane v registru nadzora dokumentov ISMS in posredovane vsem zadevnim razvojnim in produktnim ekipam.

9.4 Nadomeščene različice morajo biti arhivirane najmanj tri leta zaradi sledljivosti, revizijske preverljivosti in podpore pri preiskovanju kršitev.

10. Povezane politike in povezave

10.1 P1 – Politika informacijske varnosti. Določa temelj za zaščito sistemov in podatkov, v okviru katerega so zahtevane kontrole na ravni aplikacij za preprečevanje nepooblaščenega dostopa, uhajanja podatkov in izkoriščanja.

10.2 P4 – Politika nadzora dostopa. Določa standarde upravljanja identitet in sej, ki jih morajo uveljavljati vse aplikacije, vključno z močno avtentikacijo, načelom najmanjših privilegijev in zahtevami glede pregleda dostopov.

10.3 P5 – Politika upravljanja sprememb. Ureja prenos aplikacijske kode in konfiguracij v produkcijska okolja ter zagotavlja blokiranje nepooblaščenih ali nepreizkušenih sprememb.

10.4 P17 – Politika varstva podatkov in zasebnosti. Od aplikacij zahteva uveljavitev varstva zasebnosti že pri načrtovanju ter zakonito ravnanje z osebnimi in občutljivimi podatki, njihovo šifriranje in hrambo v vseh okoljih.

10.5 P24 – Politika varnega razvoja. Določa širši okvir za vgrajevanje varnosti v SDLC, pri čemer ta politika opredeljuje konkretne zahteve in tehnične kontrole, ki jih je treba implementirati na ravni aplikacij.

10.6 P30 – Politika odzivanja na incidente. Določa strukturirano obravnavo varnostnih incidentov aplikacij, vključno z ranljivostmi, ugotovljenimi po uvedbi ali med penetracijskim testiranjem, ter opredeljuje postopke eskalacije, zajezitve in obnovitve.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001:2022

11.1.1 Klavzula 8.1 – operativno načrtovanje in nadzor: zahteva, da se varnost aplikacij vgradi v procese in sisteme za zagotavljanje zaupnosti, celovitosti in razpoložljivosti.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroli 8.25–8.26: podrobno določata pričakovanja glede varnosti na ravni aplikacij, vključno s praksami varnega razvoja kode, modeliranjem groženj, arhitekturnimi kontrolami in preverjanjem programske opreme tretjih oseb.

11.2.2 Dodatek A, kontrola 8.25 – življenjski cikel varnega razvoja: zahteva vključitev varnosti v celoten življenjski cikel aplikacije.

11.2.3 Dodatek A, kontrola 8.26 – zahteve informacijske varnosti aplikacij: zahteva opredelitev in uveljavljanje tehničnih kontrol za zaščito aplikacij pred neustrezno uporabo in kompromitacijo.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – varnostno testiranje in vrednotenje razvijalcev: zahteva statično, dinamično in penetracijsko testiranje med razvojem.

11.3.2 SA-15 – razvojni proces, standardi in orodja: določa formalne standarde za varen razvoj aplikacij.

11.3.3 SI-10 – preverjanje vhodnih podatkov: zahteva kontrolne mehanizme za preprečevanje napadov z vbrizgavanjem in napadov pri razčlenjevanju.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 25 – varstvo podatkov že pri načrtovanju in privzeto: zahteva vključitev varstva podatkov in zasebnosti v logiko aplikacij in delovne tokove.

11.4.2 Člen 32 – varnost obdelave: zahteva ustrezne tehnične ukrepe, kot so preverjanje vhodov, šifriranje in varne kontrole dostopa.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(f): zahteva obravnavo ranljivosti in prakse varnega življenjskega cikla aplikacij za bistvene in pomembne subjekte.

11.5.2 Člen 23 – poročanje o varnostnih incidentih: zahteva zmogljivosti beleženja in spremljanja na ravni aplikacij za zaznavanje in poročanje o pomembnih incidentih.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – upravljanje tveganj IKT: finančnim subjektom nalaga, da zagotovijo varnost, preizkušenost in odpornost aplikacij proti kibernetskim grožnjam.

11.6.2 Člen 11 – testiranje orodij IKT: spodbuja periodično penetracijsko testiranje in vaje rdeče ekipe za kritične aplikacije in storitve.

11.7 COBIT 2019

11.7.1 BAI03 – upravljanje identifikacije in izgradnje rešitev: določa zahteve za zasnovo in kontrole med razvojem aplikacij.

11.7.2 BAI09 – upravljanje aplikacij: poudarja varno vzdrževanje, spremljanje in nadgrajevanje delujočih aplikacij.

11.7.3 DSS05 – upravljanje varnostnih storitev: povezuje zaščito aplikacij s širšimi organizacijskimi varnostnimi operacijami in kontrolami.