					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P28					Naslov dokumenta: **Politika zunanjega 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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8.1	N/A
ISO/IEC 27002:2022	Kontrole 5.19-5.22, 8	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
Uredba EU GDPR	Člena 28, 32	N/A
Direktiva EU NIS2	Členi 21(2)(a), (h), 23	N/A
Uredba EU DORA	Členi 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS05	N/A

1. Namen

1.1 Ta politika določa obvezne kontrole za zunanje izvajanje razvoja programske opreme ali sistemov pri zunanjih dobaviteljih, pogodbenih izvajalcih ali agencijah ter zagotavlja, da so varne prakse vključene v celoten življenjski cikel razvoja.

1.2 Njen namen je preprečiti varnostne ranljivosti, izgubo podatkov, izpostavljenost intelektualne lastnine (IP) in kršitve skladnosti, ki izhajajo iz zunanjega razvoja.

1.3 Ta politika določa upravljanje dobaviteljev, standarde varnega razvoja kode, upravljanje dostopa, obveznosti spremljanja ter postopek izstopa ob zaključku pogodbe, da se zagotovijo zaupnost, celovitost in razpoložljivost razvite programske opreme.

2. Področje uporabe

2.1 Ta politika velja za vse organizacijske enote, ki vključujejo zunanje subjekte za razvoj programske opreme ali sistemov, vključno z:

2.1.1 spletnimi aplikacijami, mobilnimi aplikacijami, vdelanimi sistemi, vmesniki za aplikacijsko programiranje, skriptami, avtomatiziranimi delovnimi tokovi ali moduli platform

2.1.2 razvojem po meri za interne platforme, sisteme za stranke ali komercialne produkte

2.1.3 sodelovanjem z razvijalci tretjih oseb, samostojnimi izvajalci, agencijami ali oddaljenimi ekipami v tujini

2.2 Ta politika ureja tudi vsak zunanji subjekt, ki med razvojem dostopa do izvorne kode, testnih okolij ali cevovodov CI/CD.

2.3 Zahteve veljajo ne glede na vrsto pogodbe, razvojno metodologijo ali geografsko lokacijo zunanjega izvajalca.

3. Cilji

3.1 Uveljaviti prakse varnega življenjskega cikla razvoja programske opreme (SDLC) v vseh zunanjih razvojnih projektih, od načrtovanja do preverjanja po uvedbi.

3.2 Zagotoviti, da vse pogodbe z zunanjimi razvijalci vključujejo obvezne klavzule o varstvu podatkov, varnem razvoju kode in zaščiti intelektualne lastnine.

3.3 Določiti zahteve glede nadzora dostopa, spremljanja in revizije za razvijalce tretjih oseb, ki sodelujejo z internimi sistemi.

3.4 Zaščititi organizacijo pred grožnjami v dobavni verigi, pravnimi kršitvami in škodo za ugled, povezano z zunanje razvito programsko opremo.

3.5 Ohraniti stalno skladnost z varnostnimi okviri, vključno z ISO/IEC 27001, NIST, GDPR, NIS2, DORA in COBIT 2019.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri visoko tvegane projekte zunanjega razvoja in potrdi izjeme od politike, kadar so utemeljene.

4.1.2 Zagotovi, da so odločitve o zunanjem izvajanju usklajene s strateškimi cilji in apetitom organizacije za tveganje.

4.2 Vodja informacijske varnosti (CISO)

4.2.1 Odobri vključitev dobaviteljev z vidika informacijske varnosti.

4.2.2 Določi zahteve glede varnostnih kontrol za zunanje izvajanje in pregleda poročila o incidentih.

[... 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 mora biti pregledana najmanj enkrat letno ali pogosteje v naslednjih primerih:

9.1.1 uvedba novih modelov zunanjega razvoja, novih dobaviteljev ali novih pristojnosti

9.1.2 posodobitve regulativnih okvirov, kot so GDPR, NIS2 ali DORA

9.1.3 po varnostnem incidentu, ki vključuje zunanjo kodo, dostop ali dobavljive rezultate

9.1.4 kot del ugotovitev notranje presoje ali izboljšav ISMS

9.2 Vodja informacijske varnosti (CISO) je odgovoren za začetek in usklajevanje pregleda politike v posvetovanju z:

9.2.1.1 pravno službo in nabavo (za uskladitev pogodbenega izvajanja)

9.2.1.2 lastniki projektov in produktov (za operativno izvedljivost)

9.2.1.3 skupino za informacijsko varnost (za posodobitve groženj in kontrol)

9.2.1.4 najvišjim vodstvom (za končno odobritev)

9.3 Vse posodobitve politike morajo biti:

9.3.1.1 upravljane z različicami in shranjene v določenem repozitoriju dokumentacije

9.3.1.2 posredovane zainteresiranim stranem, ki sodelujejo pri dejavnostih zunanjega razvoja

9.3.1.3 povezane z vsemi posodobitvami povezanih politik ali procesne dokumentacije

9.4 Vsako različico politike mora spremljati evidenca sprememb, ki zagotavlja sledljivost sprememb in odobritev.

10. Povezane politike in povezave

10.1 Ta politika podpira naslednje povezane dokumente in je z njimi povezana:

10.1.1 P1 - Politika informacijske varnosti: določa varnostna načela na ravni organizacije, ki veljajo v internih razvojnih okoljih in pri razvoju tretjih oseb.

10.1.2 P5 - Politika upravljanja sprememb: zagotavlja, da so vse spremembe, povezane z uvajanjem kode iz zunanjih repozitorijev, pregledane in odobrene pred izvedbo.

10.1.3 P13 - Politika klasifikacije in označevanja podatkov: določa, kako se občutljivi podatki opredelijo, preden so razkriti razvojnim dobaviteljem ali repozitorijem.

10.1.4 P18 - Politika kriptografskih kontrol: določa, kako je treba med razvojem in dobavo ravnati s ključi, skrivnostmi in občutljivimi prijavnimi podatki.

10.1.5 P24 - Politika varnega razvoja: določa osnovne zahteve za interne in zunanje prakse razvoja programske opreme.

10.1.6 P30 - Politika odzivanja na incidente: ureja, kako se kršitve ali varnostna vprašanja, povezana z zunanjim razvojem, eskalirajo, preiskujejo in razrešujejo.

10.1.7 P33 - Politika spremljanja presoje in skladnosti: določa zahteve za pregledovanje dejavnosti zunanjega razvoja med presojami ali pregledi skladnosti.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi varnostnimi okviri in predpisi za zagotavljanje varnega zunanjega izvajanja razvoja programske opreme ter praks upravljanja dobaviteljev.

11.2 ISO/IEC 27001

11.2.1 Klavzula 8.1 - Operativno načrtovanje in nadzor: določa procesne kontrole za varen razvoj in dobavo s strani tretjih oseb.

11.3 ISO/IEC 27002:2022 - Kontrole 5.19 do 5.21, 8.

11.3.1 Priloga A, Kontrola 5.19 - upravljanje odnosov z dobavitelji: zahteva formalne sporazume z varnostnimi in skladnostnimi klavzulami.

11.3.2 Priloga A, Kontrola 5.20 - obravnava informacijske varnosti v pogodbah z dobavitelji: zagotavlja, da so v pogodbe vključene kontrole, specifične za razvoj.

11.3.3 Priloga A, Kontrola 5.21 - upravljanje izvajanja storitev dobaviteljev: vključuje spremljanje dobavljivih rezultatov in tveganj razvoja tretjih oseb.

11.3.4 Priloga A, Kontrola 8.27 - zunanji razvoj: zahteva določene varnostne zahteve in nadzor dostopa nad zunanje razvito programsko opremo.

11.3.5 Te kontrole določajo strukturirane zahteve za izbor, pogodbeno ureditev in nadzor zunanjih razvijalcev, vključno s praksami varnega razvoja, ravnanjem s kodo in preverjanjem uspešnosti.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - Postopek nabave: zahteva, da se zahteve varnega razvoja določijo že ob nabavi.

11.4.2 SA-9 - Storitve zunanjih sistemov: ureja, kako razvijalci tretjih oseb varno sodelujejo z internimi storitvami.

11.4.3 SA-10 - upravljanje konfiguracije razvijalca: usklajeno z obveznostmi glede nadzora različic, dostopa do kode in sledljivosti sprememb za zunanje ekipe.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 28 - obveznosti obdelovalca: zahteva, da pogodbe z razvijalci tretjih oseb opredelijo zahteve glede varnosti, kontrol in revizije za ravnanje z osebnimi podatki.

11.5.2 Člen 32 - varnost obdelave: zahteva ustrezne zaščitne ukrepe (npr. šifriranje, nadzor dostopa) pri razvoju sistemov, ki obdelujejo osebne podatke.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Členi 21(2)(a), (h), 23: zahtevajo, da se prakse varnega razvoja uporabljajo pri sodelovanju s tretjimi osebami in v digitalnih dobavnih verigah, skupaj z nadzorom in tehničnim preverjanjem.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Členi 28(1), (2): zahtevajo, da finančni subjekti upravljajo tveganja IKT tretjih oseb s pogodbenimi kontrolami in nadzorom varnega razvoja, zlasti pri kritičnem zunanjem razvoju.

11.8 COBIT 2019

11.8.1 APO10 - Upravljanje dobaviteljev: določa strukturirane zahteve za ocenjevanje dobaviteljev, pogodbe in spremljanje uspešnosti.

11.8.2 BAI03 - Upravljanje izgradnje rešitev: neposredno se povezuje s procesi varnega SDLC, pregledi kode in preverjanjem razvoja.

11.8.3 DSS05 - Upravljanje varnostnih storitev: usklajeno s spremljanjem in zaščito sistemov, razvitih zunaj organizacije ali s strani tretjih oseb.