					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P28S					Naslov dokumenta: **Politika zunanjega razvoja programske opreme**							
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	Klavzule 5.1, 6.1, 8	Ustrezne kontrole ISMS ter kontrole, povezane z dobavitelji
ISO/IEC 27002:2022	Kontrole 5.19, 5.20, 8.25–8.27	Kontrole dobaviteljev in varnega življenjskega cikla razvoja
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Zahteve glede nabave, dobavne verige, varnega razvoja in sporazumov z dobavitelji
Uredba EU GDPR	Člen 28	Pogodbene zahteve in zahteve varstva podatkov za obdelavo s strani tretjih oseb
Direktiva EU NIS2	Člen 21(2)(a), (h)	Kontrole dobavne verige in varnega razvoja aplikacij
Uredba EU DORA	Člen 10	Upravljanje tveganj IKT tretjih oseb, vključno z zunanjim razvojem
COBIT 2019	BAI03, DSS05	Zahteve za zunanji razvoj in zunanje ponudnike storitev IT

1. Namen

1.1 Ta politika zagotavlja, da se ves zunanji razvoj programske opreme, ne glede na to, ali ga izvajajo samostojni izvajalci, agencije ali ponudniki storitev tretjih oseb, izvaja varno, pogodbeno urejeno ter v skladu z veljavnimi pravnimi, regulativnimi in revizijskimi zahtevami.

1.2 Organizacijo varuje pred tveganji, povezanimi z nevarno izvorno kodo, nejasnim lastništvom, izpostavljenostjo podatkov in neustreznim upravljanjem dobaviteljev, tako da določa izvršljive razvojne standarde in nadzor nad dobavitelji tudi v odsotnosti namenskega oddelka IT.

1.3 Ta politika podpira certificiranje po ISO/IEC 27001:2022 z jasno opredeljenimi pričakovanji glede razvoja, odgovornostmi in dokumentiranimi kontrolami nad razvojnimi dejavnostmi tretjih oseb.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zunanje razvijalce, vključno s samostojnimi izvajalci in razvojnimi agencijami,

2.1.2 vsa razvojna dela, ki vključujejo notranja orodja, javno dostopna spletna mesta, programske aplikacije ali poslovno avtomatizacijo,

2.1.3 osebje, odgovorno za izbor, upravljanje ali nadzor zunanjih razvijalcev,

2.1.4 vse integracije sistemov tretjih oseb, skriptiranje ali razvoj, ki so v interakciji s podatki ali sistemi podjetja.

2.2 Vključuje tudi vsako osebo ali platformo, ki ima dostop do prijavnih poverilnic podjetja, podatkovnih repozitorijev, repozitorijev izvorne kode, testnih okolij ali produkcijskih sistemov.

3. Cilji

3.1 Zagotoviti, da ves zunanji razvoj upošteva načela varnega razvoja kode in da so razvijalci pogodbeno zavezani k upoštevanju dokumentiranih standardov in določil o zaupnosti.

3.2 Vzpostaviti lastništvo nad vsemi projektnimi izdelki, vključno z izvorno kodo, sredstvi, poverilnicami in dokumentacijo, ter zagotoviti popoln prenos pravic na podjetje in sledljivo primopredajo ob zaključku projekta.

3.3 Preprečiti pogosta razvojna tveganja, vključno s ponovno uporabo lastniške kode, napadi na dobavno verigo prek knjižnic, uporabo nepodprtih ogrodij in nepreverjenim administrativnim dostopom.

3.4 Zahtevati dokumentacijo pred začetkom sodelovanja za vsak zunanji projekt, vključno s pogodbami, sporazumom o nerazkrivanju informacij in minimalnimi varnostnimi pričakovanji.

3.5 Varovati evidence o strankah, sisteme in notranje procese z doslednim nadzorom razvoja, testiranjem po dobavi in varnim upravljanjem sistemskega dostopa.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Odobri vsa razmerja z dobavitelji in podpisuje razvojne pogodbe.

4.1.2 Zagotovi, da se ves zunanji razvoj izvaja v skladu s to politiko.

4.1.3 Po zaključku projekta odstrani dostop do sistemov podjetja.

4.1.4 Pregleda dokumentacijo in rezultate po dobavi.

4.2 Lastnik projekta (običajno notranji zaposleni ali imenovani koordinator)

4.2.1 Upravlja dnevno koordinacijo z zunanjim razvijalcem.

4.2.2 Preveri, da so funkcionalne zahteve izpolnjene in da so dobave testirane.

4.2.3 Zagotovi varno predajo izvorne kode in poverilnic.

4.2.4 Generalnemu direktorju poroča o vseh težavah ali incidentih, povezanih z razvojem.

[... 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 Letni pregled

9.1.1 To politiko mora generalni direktor (GM) pregledati najmanj enkrat letno. Pregled zagotavlja, da politika še naprej izpolnjuje:

9.1.1.1 zahteve za certificiranje po ISO/IEC 27001,

9.1.1.2 spremembe pravnih obveznosti (npr. člen 28 GDPR, člen 10 DORA),

9.1.1.3 aktualne razvojne prakse na ravni MSP in tveganja tretjih oseb.

9.2 Vmesni pregledi

9.2.1 Pregled politike se mora izvesti tudi, kadar:

9.2.1.1 se v uporabo uvede nov dobavitelj ali platforma za zunanji razvoj,

9.2.1.2 pride do pomembnega incidenta, povezanega z zunanjim razvojem,

9.2.1.3 nastopijo bistvene spremembe v uporabljenih orodjih, platformah ali okoljih.

9.3 Postopek pregleda

9.3.1 Generalni direktor je odgovoren za:

9.3.1.1 preverjanje, da pogodbe, sporazumi o nerazkrivanju informacij in procesi nadzora dostopa ostajajo učinkoviti,

9.3.1.2 potrditev, da so trenutni dobavitelji in samostojni izvajalci usklajeni s politiko,

9.3.1.3 posodobitev določb na podlagi povratnih informacij iz preteklih projektov ali incidentov.

9.4 Nadzor različic in obveščanje

9.4.1 Vse spremembe morajo biti:

9.4.1.1 zabeležene z datumom, razlogom in opisom spremembe,

9.4.1.2 odobrene s strani generalnega direktorja in dodane v evidenco različic,

9.4.1.3 sporočene vsem zaposlenim ali lastnikom projektov, ki sodelujejo z zunanjimi razvijalci,

9.4.1.4 po potrebi ponovno posredovane vsem zadevnim dobaviteljem in tretjim osebam.

10. Povezane politike in povezave

10.1 Ta politika neposredno podpira izvajanje naslednjih politik, usklajenih z MSP, in je od njih odvisna:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: pojasnjuje, kdo je odgovoren za odobritev dobaviteljev, nadzor dostopa in sprejemanje tveganja pri uporabi zunanjih razvijalcev.

10.1.2 P4S – Politika nadzora dostopa: določa pravilno vzpostavitev, omejevanje in ukinitev uporabniških računov ter administratorskega dostopa, uporabljenih pri zunanjem razvoju.

10.1.3 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da notranje osebje razume, kako varno koordinirati delo z zunanjimi razvijalci, vključno z ravnanjem s poverilnicami in projektnimi datotekami.

10.1.4 P17S – Politika varstva podatkov in zasebnosti: določa varnostne in pravne zahteve za ravnanje z osebnimi podatki, ki jih lahko zunanji razvijalci obdelujejo v skladu z GDPR.

10.1.5 P24S – Politika varnega razvoja: določa, kako morata notranji in zunanji razvoj upoštevati prakse varnega razvoja kode ter preverjanje knjižnic in ogrodij.

10.1.6 P30S – Politika odzivanja na incidente: uporablja se, kadar zunanji razvoj povzroči varnostne incidente ali ranljivosti, ter usmerja usklajeno preiskavo in odpravo pomanjkljivosti.

10.2 Te politike se morajo izvajati vzporedno, da zunanji razvoj ne ustvarja neobvladovanega tveganja ali ne povzroča neskladnosti z obveznostmi MSP.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1 – Organizacije morajo oceniti in obravnavati tveganja informacijske varnosti, povezana z dobavitelji.

11.1.2 Klavzula 8.1 – Zahteva operativno načrtovanje in nadzor, vključno s storitvami tretjih oseb, kot je zunanji razvoj.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – Priporoča oceno sposobnosti dobaviteljev za izpolnjevanje zahtev informacijske varnosti.

11.2.2 Kontrola 5.20 – Spodbuja redno spremljanje in periodični pregled storitev tretjih oseb.

11.2.3 Kontrole 8.25–8.27 – Opredeljujejo prakse varnega življenjskega cikla razvoja, ki se uporabljajo tudi za zunanji razvoj.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Zahteva, da strategije nabave vključujejo ukrepe informacijske varnosti.

11.3.2 SA-9 – Obravnava zunanji razvoj sistemov in tveganja dobavne verige.

11.3.3 SA-11 – Določa prakse varnega razvoja, vključno s pregledom izvorne kode in odpravo pomanjkljivosti.

11.3.4 SA-15 – Spodbuja uporabo avtomatiziranih orodij za zaznavanje pomanjkljivosti in zagotavljanje programske opreme.

11.3.5 SR-3 – Zahteva, da sporazumi z dobavitelji vključujejo zahteve glede kibernetske varnosti.

11.4 Splošna uredba EU o varstvu podatkov (GDPR)

11.4.1 Člen 28 – Zahteva pogodbe s podobdelovalci ali drugimi tretjimi osebami, ki zagotavljajo ustrezne zaščitne ukrepe varstva podatkov, kar se neposredno uporablja za razvijalce, ki obdelujejo ali dostopajo do osebnih podatkov.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a), (h) – Zahteva kontrole varnosti dobavne verige in prakse varnega razvoja programske opreme za zavezane ponudnike digitalnih storitev, vključno z MSP, kadar je to relevantno.

11.6 Uredba EU o digitalni operativni odpornosti (DORA)

11.6.1 Člen 10 – Zahteva upravljanje tveganj IKT tretjih oseb, vključno z razvojnimi pogodbami, varnostnimi obveznostmi in kontrolami tveganj, povezanimi s ponudniki tretjih oseb.

11.7 COBIT 2019

11.7.1 BAI03 – Upravljanje identifikacije in izgradnje rešitev – zagotavlja, da zunanji razvoj izpolnjuje poslovne zahteve in varnostna pričakovanja.

11.7.2 DSS05 – Upravljanje varnostnih storitev – zahteva, da zunanji ponudniki varnostnih storitev in razvojni izvajalci delujejo v skladu z uveljavljenimi varnostnimi pravili in nadzorom.