					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P26S					Naslov dokumenta: **Politika varnosti tretjih oseb in dobaviteljev**							
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	Operativne kontrole za odnose s tretjimi osebami in dobavitelji
ISO/IEC 27002:2022	Kontrole 5.19–5.22	Kontrole varnosti dobaviteljev, pogodbena varnostna določila, upravljanje sprememb, spremljanje in pregled
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Nabava, konfiguracija, sporazumi o medsebojni povezavi in kontrole za zunanje osebje
EU GDPR	Člena 28, 32	pogodba o obdelavi osebnih podatkov, varnostne zahteve za obdelovalce
EU NIS2	Členi 21(2)(a)(b)(i), 23(1)	upravljanje tveganj v dobavni verigi, nadzor nad storitvami tretjih oseb
EU DORA	Členi 5(1)(2), 28(1)(2)	upravljanje tveganj IKT pri ponudnikih storitev tretjih oseb
COBIT 2019	APO10, APO12, DSS05	upravljanje dobaviteljev in vključevanje tveganj

1. Namen

1.1 Ta politika določa obvezne varnostne zahteve za vzpostavljanje, upravljanje in prenehanje odnosov s tretjimi osebami in dobavitelji, ki dostopajo do podatkov, sistemov ali storitev organizacije ali nanje vplivajo.

1.2 Zagotavlja, da zunanji ponudniki, vključno s ponudniki IT-podpore, ponudniki storitev v oblaku, razvijalci programske opreme in izvajalci poslovnih procesov, varno ravnajo s sredstvi podjetja ter delujejo skladno z veljavno zakonodajo in standardi.

1.3 Ta politika zmanjšuje tveganja, kot so razkritje podatkov, nepooblaščene spremembe sistemov, regulatorne globe ali prekinitve poslovanja, ki nastanejo zaradi neustrezno varovanih ali slabo upravljanih odnosov s tretjimi osebami.

2. Področje uporabe

2.1 Ta politika velja za vse tretje osebe, ki:

2.1.1 zagotavljajo programsko opremo, infrastrukturo, gostovanje ali storitve v oblaku,

2.1.2 dostopajo do notranjih sistemov, naprav ali aplikacij ali jih upravljajo,

2.1.3 obdelujejo podatke podjetja, dokumente ali varnostne kopije,

2.1.4 podpirajo poslovanje, kadrovsko funkcijo, finance ali storitve za stranke.

2.2 Velja tudi za:

2.2.1 notranje osebje, vključeno v izbiro, angažiranje ali nadzor dobaviteljev,

2.2.2 vse osebe, ki upravljajo uvajanje dobaviteljev, pogodbe, dostope ali preglede,

2.2.3 vsak sistem ali proces, ki je odvisen od komponent ali storitev tretjih oseb.

3. Cilji

3.1 Zagotoviti, da vsi dobavitelji izpolnjujejo jasno določene varnostne zahteve.

3.2 Zahtevati, da pogodbe z dobavitelji vključujejo izvršljive obveznosti glede varnosti, zasebnosti in odzivanja na incidente.

3.3 Oceniti in dokumentirati tveganja dobaviteljev pred podpisom pogodbe ali dodelitvijo dostopa.

3.4 Izvajati redne preglede kritičnih dobaviteljev ali dobaviteljev z visokim tveganjem za potrditev skladnosti.

3.5 Vzpostaviti formalen postopek za izjeme, upravljanje incidentov in posodobitve pogodb.

3.6 Podpreti skladnost z zahtevami standarda ISO/IEC 27001:2022, GDPR, NIS2 in DORA, ki se nanašajo na upravljanje dobaviteljev.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 nosi končno odgovornost za izbiro dobaviteljev in skladnost z varnostnimi zahtevami,

4.1.2 odobri pogodbe, izjeme in eskalacije, povezane z dobavitelji,

4.1.3 nadzira odzivanje na incidente in odločanje v primerih, ko dobavitelji ne izpolnijo svojih obveznosti.

4.2 Ponudnik IT-podpore ali notranja kontaktna oseba za informacijsko varnost

4.2.1 ocenjuje tehnični dostop, ki ga zahtevajo dobavitelji,

4.2.2 določa pravila nadzora dostopa, pregleduje dnevnike in preverja varno ravnanje s podatki,

4.2.3 pregleduje dokazila o varnostnih kontrolah, potrdila o informacijski varnosti ali rezultate presoj, kadar je to ustrezno.

[... 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 najmanj enkrat letno pregledati generalni direktor ob sodelovanju ponudnika IT-podpore ali odgovorne osebe za upravljanje dobaviteljev.

9.2 Politiko je treba pregledati tudi:

9.2.1 po vsaki pomembni spremembi zakonskih, regulatornih ali pogodbenih obveznosti,

9.2.2 po varnostnem incidentu ali ugotovitvi presoje, povezani z dobaviteljem,

9.2.3 ob uvedbi novih kategorij dobaviteljev (npr. kritične platforme SaaS).

9.3 Vse posodobitve morajo biti:

9.3.1 dokumentirane z evidenco različic in utemeljitvijo,

9.3.2 odobrene s strani generalnega direktorja,

9.3.3 sporočene ustreznemu notranjemu osebju in osebam, odgovornim za upravljanje dobaviteljev,

9.3.4 hranjene skupaj s prejšnjimi različicami v skladu s P14S – Politika hrambe podatkov in odstranjevanja.

10. Povezane politike in povezave

10.1 Učinkovitost te politike je odvisna od usklajenosti z naslednjimi politikami informacijske varnosti za MSP:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornost za nadzor nad dobavitelji in uveljavljanje pogodbenih določil.

10.1.2 P4S – Politika nadzora dostopa: določa pravila omejevanja dostopa, ki jih je treba uporabljati, kadar dobavitelji pridobijo dostop do sistemov.

10.1.3 P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da dobavitelji, ki obdelujejo osebne podatke, ravnajo skladno z načeli varstva podatkov in pravnimi zahtevami.

10.1.4 P14S – Politika hrambe podatkov in odstranjevanja: velja za vse podatke ali evidence, deljene z dobavitelji ali hranjene pri njih, in ureja varno odstranjevanje po prenehanju pogodbe.

10.1.5 P30S – Politika odzivanja na incidente: določa način odzivanja, kadar dobavitelj povzroči varnostni incident ali je vanj vključen, vključno z eskalacijo in postopki ravnanja z dokazi.

10.2 Te politike skupaj zagotavljajo, da se tveganja, povezana z dobavitelji, obvladujejo skozi celoten življenjski cikel pogodbe.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – zahteva izvajanje operativnih kontrol, vključno s tistimi, ki se uporabljajo za odnose s tretjimi osebami in dobavitelji.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – zagotavlja, da so varnostni ukrepi dobaviteljev usklajeni z zahtevami organizacije.

11.2.2 Kontrola 5.20 – zahteva formalne sporazume, ki vključujejo varnostna določila, odgovornosti in obveznosti ob kršitvah.

11.2.3 Kontrola 5.21 – ureja spremembe pri storitvah dobaviteljev, ki lahko vplivajo na profil varnostnega tveganja.

11.2.4 Kontrola 5.22 – zahteva spremljanje in pregled storitev dobaviteljev ter skladnosti.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – ureja nabavo zunanjih sistemov in storitev ter zahteva ocene tveganja in jasno določena pričakovanja.

11.3.2 SA-10 – ureja konfiguracijo in postopke sprememb, ki vključujejo sisteme v upravljanju tretjih oseb.

11.3.3 CA-3 – zahteva sporazume o medsebojni povezavi sistemov, ki vključujejo zunanje subjekte.

11.3.4 PS-7 – določa preverjanje in odgovornost za zunanje osebje.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 28 – zahteva pogodbo o obdelavi osebnih podatkov z dobavitelji, ki nastopajo kot obdelovalci.

11.4.2 Člen 32 – zahteva ustrezne tehnične in organizacijske varnostne ukrepe za vse obdelovalce.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(a), (b), (i) – zahteva upravljanje tveganj IKT v dobavni verigi in kontrole tretjih oseb.

11.5.2 Člen 23(1) – zahteva dokumentiran nadzor nad storitvami tretjih oseb za bistvene in pomembne subjekte.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 5(1) – zahteva okvir upravljanja tveganj IKT, ki zajema vse kritične zunanje ponudnike.

11.6.2 Člen 5(2) – določa pogodbene in operativne kontrole za odvisnosti od storitev IKT.

11.6.3 Člen 28(1), (2) – vzpostavlja pravila nadzora nad tveganji IKT tretjih oseb v finančnem sektorju.

11.7 COBIT 2019

11.7.1 APO10 – »Upravljanje dobaviteljev« opredeljuje nabavne kontrole in pričakovanja glede upravljanja odnosov.

11.7.2 APO12 – »Upravljanje tveganj« vključuje tveganja dobaviteljev v upravljanje organizacijskih tveganj.

11.7.3 DSS05 – »Upravljanje varnostnih storitev« velja za upravljane tretje osebe in zunanje izvajalce storitev.