					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P26					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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Operativno načrtovanje in nadzor: zahteva formalne kontrole nad storitvami tretjih oseb, ki vplivajo na ISMS
ISO/IEC 27002:2022	Kontrole 5.19–5.22	Politike in postopki za odnose z dobavitelji; upravljanje tveganj dobaviteljev; upravljanje izvajanja storitev dobaviteljev; spremljanje in pregled dobaviteljev
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Zunanje sistemske storitve; upravljanje konfiguracije pri razvoju; medsebojne povezave sistemov; varnost osebja tretjih oseb
Uredba (EU) GDPR	Členi 28, 32, 33	Obveznosti obdelovalca, varnost obdelave, obveščanje o kršitvi varnosti osebnih podatkov
Direktiva (EU) NIS2	Člen 21(2)(e–f)	upravljanje dobaviteljev na podlagi tveganj in varnostni nadzor
Uredba (EU) DORA	Členi 28, 30	tveganja IKT, povezana s tretjimi osebami, ter nadzor nad kritičnimi zunanjimi ponudniki storitev IKT
COBIT 2019	BAI05, DSS02, MEA03	Upravljanje omogočanja organizacijskih sprememb; upravljanje zahtevkov za storitve in incidentov; spremljanje, vrednotenje in ocenjevanje skladnosti

1. Namen

1.1 Ta politika določa zahteve informacijske varnosti za vzpostavitev, upravljanje in vzdrževanje varnih odnosov s tretjimi dobavitelji in ponudniki storitev.

1.2 Zagotavlja, da za vse dobavitelje z dostopom do podatkov, sistemov ali infrastrukture organizacije veljajo stroge varnostne kontrole, pogodbena zaščita in stalni nadzor v celotnem življenjskem ciklu storitve.

1.3 Politika podpira kontrole 5.19 do 5.22 iz Priloge A standarda ISO/IEC 27001 z vključevanjem varnostnih zahtev v nabavo, uvajanje, skrbni pregled dobaviteljev, upravljanje pogodb, spremljanje storitev in postopke prenehanja sodelovanja.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse tretje dobavitelje, pogodbene izvajalce, ponudnike storitev v oblaku in storitvene organizacije, ki obdelujejo informacijska sredstva organizacije ali do njih dostopajo,

2.1.2 vse notranje vloge, vključene v ocenjevanje dobaviteljev, uvajanje dobaviteljev, sklepanje pogodb, obvladovanje tveganj, spremljanje ali prenehanje sodelovanja,

2.1.3 vse odnose z dobavitelji, ki vključujejo dostop do občutljivih podatkov, integracijo s produkcijskimi storitvami ali podporo poslovno kritičnim funkcijam.

2.2 Zajema neposredne dobavitelje in njihove podizvajalce, kadar je to ustrezno, ter vključuje programsko opremo tretjih oseb, infrastrukturo, podporo in upravljane storitve.

3. Cilji

3.1 Zagotoviti, da se varnostna tveganja, povezana z dobavitelji, dosledno prepoznavajo, ocenjujejo in zmanjšujejo v celotnem življenjskem ciklu odnosa.

3.2 V vse pogodbe z dobavitelji vključiti standardizirane varnostne zahteve, vključno z obveznostmi obveščanja o kršitvah, določili o pravici do revizije in odgovornostmi glede varstva podatkov.

3.3 Zahtevati formalni skrbni pregled dobaviteljev in dokumentirane ocene tveganja pred vključitvijo novih dobaviteljev ali obnovitvijo pogodb o storitvah z visokim tveganjem.

3.4 Vzpostaviti mehanizme za stalno spremljanje skladnosti dobaviteljev, vključno s pregledi uspešnosti, revizijami in eskalacijo incidentov.

3.5 Upravljati spremembe storitev dobaviteljev ter ob prenehanju sodelovanja zagotoviti varen postopek izstopa in vračilo oziroma uničenje podatkov.

3.6 Uskladiti varnostne kontrole tretjih oseb z veljavnimi regulativnimi in pogodbenimi obveznostmi, vključno z GDPR, NIS2, DORA in standardom ISO/IEC 27001.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik te politike in zagotavlja njeno usklajenost s celotnim sistemom upravljanja informacijske varnosti (ISMS), obvladovanjem tveganj in strategijo skladnosti.

4.1.2 Odobrava razrede razvrstitve dobaviteljev, rezultate varnostnih pregledov in izjeme z visokim tveganjem.

4.1.3 Sodeluje pri eskalaciji resnih incidentov, povezanih z dobavitelji, in pri pogodbenih pogajanjih za kritične storitve.

4.2 Nabava in upravljanje dobaviteljev

4.2.1 Zagotavlja, da vse nove in obnovljene pogodbe z dobavitelji vključujejo odobrena varnostna določila in določila o varstvu podatkov.

4.2.2 Vzdržuje centralno evidenco dobaviteljev in se usklajuje s funkcijo pravnih zadev in skladnosti glede dokumentacije tveganj tretjih oseb.

4.2.3 Začne postopke uvajanja dobaviteljev in zagotavlja usklajenost s predpogodbenimi varnostnimi presojami.

[... 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 najmanj enkrat letno ali prej v primeru:

9.1.1 bistvenih sprememb nabavne strategije ali ekosistema dobaviteljev,

9.1.2 posodobitev pravnih ali regulativnih okvirov (npr. DORA, GDPR),

9.1.3 večjih incidentov tretjih oseb, kršitev varnosti osebnih podatkov ali neuspešnih revizij,

9.1.4 ugotovitev iz ocen tveganja ali ugotovitev zunanjih certifikacijskih organov.

9.2 Za postopek pregleda so skupaj odgovorni vodja informacijske varnosti (CISO), nabava, pravna služba in funkcija obvladovanja tveganj.

9.3 Vse spremembe politike morajo biti dokumentirane v registru nadzora dokumentov ISMS, vodene pod nadzorom različic in sporočene ustreznim zainteresiranim stranem prek kanalov upravljanja dobaviteljev in programov ozaveščanja zaposlenih.

9.4 Nadomeščene različice morajo biti zaradi sledljivosti in pravne skladnosti arhivirane najmanj tri leta.

10. Povezane politike in povezave

10.1 P1 – Politika informacijske varnosti. Določa krovno zavezanost varovanju vseh dejavnosti organizacije, vključno z odvisnostjo od tretjih dobaviteljev in zunanjih ponudnikov storitev.

10.2 P6 – Politika upravljanja tveganj. Usmerja prepoznavanje, ocenjevanje in zmanjševanje tveganj, povezanih z odnosi s tretjimi osebami, vključno s podedovanimi ali sistemskimi tveganji iz ekosistema dobaviteljev.

10.3 P17 – Politika varstva podatkov in zasebnosti. Uporablja se za vse dobavitelje, ki obdelujejo osebne podatke, ter zahteva ustrezna pogodbena določila, zaščitne ukrepe pri prenosu in načela vgrajenega varstva zasebnosti.

10.4 P4 – Politika nadzora dostopa. Ureja, kako osebje tretjih oseb pridobi dostop do sistemov organizacije, ter uveljavlja dovoljenja na podlagi vlog, nadzor sej in postopke preklica.

10.5 P22 – Politika beleženja in spremljanja. Zahteva, da se dostop dobaviteljev do sistemov spremlja, beleži in pregleduje, zlasti v okoljih, kjer potekajo privilegirane dejavnosti ali dejavnosti, povezane s podatki.

10.6 P30 – Politika odzivanja na incidente. Določa postopke eskalacije in zahteve glede poročanja o kršitvah za varnostne dogodke, ki izvirajo od dobaviteljev, ali za skupne preiskave, ki vključujejo sisteme tretjih oseb.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001: Klavzula 8.1 – Operativno načrtovanje in nadzor: zahteva formalne kontrole nad storitvami tretjih oseb, ki vplivajo na ISMS.

11.2 ISO/IEC 27002:2022 – Kontrole 5.19 do 5.22:

11.2.1 Kontrola 5.19 iz Priloge A – Politike in postopki za odnose z dobavitelji: zahteva kontrole za upravljanje interakcij z dobavitelji.

11.2.2 Kontrola 5.20 iz Priloge A – Upravljanje tveganj dobaviteljev: osredotoča se na prepoznavanje, ocenjevanje in stalni nadzor nad profilom tveganja na področju varnosti pri dobaviteljih.

11.2.3 Kontrola 5.21 iz Priloge A – Upravljanje izvajanja storitev dobaviteljev: zahteva usklajenost izvajanja storitev in varnosti s pogodbenimi pričakovanji.

11.2.4 Kontrola 5.22 iz Priloge A – Spremljanje in pregled dobaviteljev: poudarja potrebo po stalnem preverjanju in ponovni presoji skladnosti tretjih oseb.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Zunanje sistemske storitve: določa varnostne zahteve in zahteve glede tveganj za sisteme, ki jih upravljajo zunanji subjekti.

11.3.2 SA-10 – Upravljanje konfiguracije pri razvoju: uporablja se, kadar tretje osebe dobavljajo programsko opremo ali okolja.

11.3.3 CA-3 – Medsebojne povezave sistemov: zahteva nadzor in dogovor o tokovih podatkov med sistemi različnih subjektov.

11.3.4 PS-7 – Varnost osebja tretjih oseb: zagotavlja, da so pogodbeni izvajalci in osebje dobaviteljev ustrezno preverjeni in nadzorovani.

11.4 Uredba (EU) GDPR (2016/679):

11.4.1 Člen 28 – Obveznosti obdelovalca: zahteva pisne dogovore z obdelovalci osebnih podatkov, vključno s tehničnimi in organizacijskimi ukrepi.

11.4.2 Člen 32 – Varnost obdelave: nalaga ustrezne zaščitne ukrepe tako upravljavcem kot obdelovalcem.

11.4.3 Člen 33 – Obveščanje o kršitvi varnosti osebnih podatkov: zahteva hitro obveščanje v primeru kršitve.

11.5 Direktiva (EU) NIS2 (2022/2555):

11.5.1 Člen 21(2)(e–f): zahteva upravljanje dobaviteljev na podlagi tveganj in varnostni nadzor, zlasti v digitalnih dobavnih verigah bistvenih in pomembnih subjektov.

11.6 Uredba (EU) DORA (2022/2554):

11.6.1 Člen 28 – Tveganja IKT, povezana s tretjimi osebami: določa obveznosti glede ocene tveganja, pogodbenih varnostnih določil in izhodnih strategij za ponudnike finančnih storitev.

11.6.2 Člen 30 – Nadzor nad kritičnimi zunanjimi ponudniki storitev IKT: vzpostavlja okrepljeno spremljanje in nadzorna pričakovanja za ključne dobavitelje.

11.7 COBIT 2019:

11.7.1 BAI05 – Upravljanje omogočanja organizacijskih sprememb: zagotavlja, da se prehodi med dobavitelji upravljajo na varen način.

11.7.2 DSS02 – Upravljanje zahtevkov za storitve in incidentov: uporablja se za težave, ki jih prijavijo dobavitelji, ter za integracijo obravnave incidentov.

11.7.3 MEA03 – Spremljanje, vrednotenje in ocenjevanje skladnosti: krepi merjenje uspešnosti dobaviteljev in spremljanje skladnosti.