					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P27					Naslov dokumenta: **Politika uporabe storitev v oblaku**							
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	Zahteve za operativno načrtovanje in nadzor storitev v oblaku.
ISO/IEC 27002:2022	Kontrole 5.23–5.25	Zahteve glede uporabe, politike in varnosti storitev v oblaku.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Uporaba zunanjih sistemov, pogodbene in tehnične zahteve, kriptografski zaščitni ukrepi, zaščita dobavne verige.
Uredba EU GDPR	Členi 28, 32, Poglavje V	Zahteve za obdelovalce v oblaku, varnost obdelave, prenose podatkov.
Direktiva EU NIS2	Člen 21(2)(f, i)	Zahteve glede tveganj tretjih oseb in dobavne verige.
Uredba EU DORA	Členi 5(2), 28	Nadzor nad sistemi IKT in tretjimi osebami (oblak) za finančne subjekte.
COBIT 2019	BAI04, DSS01, DSS05	Razpoložljivost storitev v oblaku, operacije, upravljanje varnosti.

1. Namen

1.1 Ta politika določa obvezne zahteve organizacije za varno, skladno in odgovorno uporabo storitev računalništva v oblaku v modelih Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) in Software-as-a-Service (SaaS).

1.2 Namen politike je zagotoviti, da se storitve v oblaku uvajajo in upravljajo na način, ki varuje zaupnost, celovitost in razpoložljivost (CIA) informacijskih sredstev ter hkrati izpolnjuje regulativne, pravne in pogodbene obveznosti.

1.3 Politika določa kontrole za obvladovanje tveganj, povezanih z oblakom, zaščito podatkov, spremljanje skladnosti ponudnikov in odpravo nepooblaščene uporabe. Hkrati podpira poslovne inovacije prek platform v oblaku z usklajevanjem varnosti, operativne zanesljivosti in stroškovne učinkovitosti.

2. Področje uporabe

2.1 Ta politika velja za vse zaposlene, pogodbene izvajalce, ponudnike storitev tretjih oseb in zunanje svetovalce, ki v imenu organizacije dodeljujejo, konfigurirajo, dostopajo do, upravljajo ali uporabljajo storitve v oblaku.

2.2 Velja za vsa okolja, v katerih se obdelujejo podatki ali delovne obremenitve organizacije, vključno z:

2.2.1 javnimi, zasebnimi, hibridnimi in skupnostnimi uvedbami v oblaku,

2.2.2 vsemi modeli storitev v oblaku (IaaS, PaaS, SaaS),

2.2.3 večoblačnimi in federativnimi arhitekturami,

2.2.4 uporabo Shadow IT ali osebnih računov v oblaku za poslovne namene.

2.3 Zajema vse ravni klasifikacije informacij in velja tako za notranje sisteme kot tudi za platforme, ki jih gostujejo dobavitelji, na katerih se hranijo ali obdelujejo podatki v lasti organizacije ali regulirani podatki.

3. Cilji

3.1 Zagotoviti varno in dosledno uporabo tehnologij v oblaku z jasno določenimi pravili uporabe, osnovnimi varnostnimi zahtevami in upravljavskimi vlogami.

3.2 Zmanjšati operativna in regulativna tveganja, povezana z računalništvom v oblaku, vključno z nepooblaščenim dostopom, kršitvami varnosti osebnih podatkov, napačno konfiguracijo, neskladnostjo in motnjami storitev.

3.3 Uveljaviti zahteve glede varnosti in zasebnosti za vse ponudnike storitev v oblaku ter preverjati skladnost s pogodbenimi določili, presojami in pravicami do revizije.

3.4 Omogočiti razširljivo in odporno uporabo oblaka brez ogrožanja profila tveganja na področju varnosti, pravnih zahtev ali neprekinjenega poslovanja.

3.5 Uskladiti upravljanje in uporabo storitev v oblaku z okvirom sistema upravljanja informacijske varnosti organizacije, pravnimi obveznostmi (npr. GDPR, DORA), sektorskimi smernicami in uveljavljenimi dobrimi praksami v panogi (npr. NIST, COBIT).

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri Politiko uporabe storitev v oblaku in strateški načrt uvajanja oblaka.

4.1.2 Pregleduje in potrjuje izjeme z visokim tveganjem od standardnih zahtev za upravljanje storitev v oblaku.

4.1.3 Zagotavlja, da pobude, povezane z oblakom, prejmejo ustrezna sredstva, nadzor in vključitev v korporativne okvire za obvladovanje tveganj.

4.2 Vodja informacijske varnosti (CISO)

4.2.1 Je lastnik te politike in organizacijskega registra storitev v oblaku.

4.2.2 Na podlagi skrbnega pregleda dobaviteljev in ocene tveganja odobri uvedbo novih ponudnikov storitev v oblaku.

4.2.3 Pregleduje dokumentacijo ponudnikov o skladnosti in potrjuje usklajenost z varnostnimi zahtevami.

[... 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 in po potrebi posodobljena, da se zagotovi stalna usklajenost z:

9.1.1 razvijajočimi se pravnimi in regulativnimi zahtevami (npr. GDPR, NIS2, DORA),

9.1.2 spremembami standardov ISO/IEC 27001 ali ISO/IEC 27002,

9.1.3 posodobitvami oblačne arhitekture organizacije, profila tveganj ali portfelja storitev,

9.1.4 preiskavami incidentov, rezultati presoj ali spoznanji iz operativne uporabe.

9.2 Za začetek pregleda in sklic ustreznih deležnikov je odgovoren vodja informacijske varnosti (CISO), vključno z:

9.2.1 varnostnim arhitektom za oblak,

9.2.2 ekipo za pravne zadeve in skladnost,

9.2.3 nabavo in upravljavci dobaviteljev,

9.2.4 lastniki storitev in IT-operacijami.

9.3 Vse posodobitve morajo biti:

9.3.1 verzionirane in datirane,

9.3.2 odobrene s strani najvišjega vodstva,

9.3.3 sporočene prizadetim stranem, vključno z zaposlenimi, pogodbenimi izvajalci in tretjimi osebami,

9.3.4 arhivirane v skladu z internimi politikami dokumentiranja.

9.4 Vmesne preglede lahko sprožijo:

9.4.1 nova sodelovanja s CSP ali večje migracije,

9.4.2 nastajajoče grožnje za infrastrukturo v oblaku,

9.4.3 bistvene spremembe pogodbenih, pravnih ali sektorskih obveznosti.

10. Povezane politike in povezave

10.1 Ta politika je tesno povezana z naslednjimi internimi politikami in je od njih odvisna:

10.1.1 P1 – Politika informacijske varnosti: Določa krovna načela za varno delovanje sistemov in storitev, ki jih ta politika uveljavlja v kontekstu oblaka.

10.1.2 P5 – Politika upravljanja sprememb: Vse spremembe konfiguracij v oblaku morajo slediti postopkom nadzora sprememb, določenim v P5.

10.1.3 P13 – Politika klasifikacije in označevanja podatkov: Določa, kako se podatki presojajo pred prenosom v oblak in kako se uporabljajo kontrole, kot sta šifriranje in lokacija hrambe.

10.1.4 P18 – Politika kriptografskih kontrol: Določa standarde za šifriranje, upravljanje ključev in uporabo kriptografskih algoritmov, ki se neposredno uporabljajo pri konfiguracijah storitev v oblaku.

10.1.5 P22 – Politika beleženja in spremljanja: Določa zahteve za zbiranje, hrambo in analizo dnevnikov, ki jih je treba uveljavljati v okoljih v oblaku.

10.1.6 P30 – Politika odzivanja na incidente: Določa postopke eskalacije, zajezitve in odpravljanja pomanjkljivosti za varnostne dogodke, povezane z oblakom.

10.1.7 P33 – Politika spremljanja presoje in skladnosti: Podpira pripravljenost na revizijo in stalno zagotovilo, da se kontrole v oblaku izvajajo in spremljajo.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001: Klavzula 8.1 – Operativno načrtovanje in nadzor: Zahteva, da organizacije uvedejo in obvladujejo procese, potrebne za izpolnjevanje zahtev informacijske varnosti, vključno s tistimi, ki vključujejo okolja v oblaku.

11.2 ISO/IEC 27002:2022 – Kontrole 5.23 do 5.25:

11.2.1 Priloga A, kontrola 5.23 – Uporaba storitev v oblaku: Zahteva presojo na podlagi tveganj, formalno odobritev in dokumentiranje uporabe storitev v oblaku.

11.2.2 Priloga A, kontrola 5.24 – Politika uporabe storitev v oblaku: Zahteva vzpostavitev in uveljavljanje formalnih politik uporabe storitev v oblaku, usklajenih s potrebami in tveganji organizacije.

11.2.3 Priloga A, kontrola 5.25 – Varnost v storitvah v oblaku: Zahteva vključitev varnosti, pogodbene zaščitne ukrepe in spremljanje delovnih obremenitev ter podatkov, gostovanih v oblaku.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Uporaba zunanjih sistemov: Zahteva določena pravila in pogoje za dostop do virov organizacije iz zunanjih sistemov ali sistemov v oblaku.

11.3.2 SA-9(5) – Storitve zunanjih informacijskih sistemov: Uveljavlja pogodbene varnostne zahteve, nadzor in stalno spremljanje za sisteme v oblaku tretjih oseb.

11.3.3 SC-12 do SC-28 – Kriptografski zaščitni ukrepi, zaščita omrežnih meja in celovitost prenosa: Usklajeni so z zahtevami glede šifriranja, identitet in dostopa za storitve, gostovane v oblaku, ter podatke med prenosom.

11.3.4 SR-5 – Zaščita dobavne verige: Podpira preverjanje in pogodbeni nadzor nad CSP, ki sodelujejo pri izvajanju storitev.

11.4 Uredba EU GDPR (2016/679):

11.4.1 Člen 28 – Obveznosti obdelovalca: Zahteva formalne pogodbe s ponudniki storitev v oblaku za zagotavljanje varnosti, zaupnosti in preverljivosti obdelave osebnih podatkov.

11.4.2 Člen 32 – Varnost obdelave: Podpira uporabo šifriranja, kontrol dostopa, beleženja in drugih zaščitnih ukrepov v okoljih v oblaku.

11.4.3 Poglavje V – Mednarodni prenosi podatkov: Uveljavlja zakonit prenos podatkov zunaj EU/EGP z uporabo zaščitnih ukrepov, kot so standardne pogodbene klavzule (SCC) ali sklepi o ustreznosti.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Člen 21(2)(f, i): Zahteva, da subjekti obvladujejo tveganja, ki izhajajo iz ponudnikov storitev v oblaku tretjih oseb, in zagotavljajo celovitost digitalne dobavne verige s pogodbenimi in tehničnimi ukrepi.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Člen 5(2) – Upravljanje tveganj IKT: Zahteva vključitev tveganj tretjih oseb na področju IKT, vključno s storitvami v oblaku, v celovito upravljanje tveganj.

11.6.2 Člen 28 – Nadzor nad kritičnimi tretjimi ponudniki IKT: Zahteva, da finančni subjekti spremljajo, nadzorujejo in poročajo o odvisnostih od ponudnikov storitev v oblaku, profilu tveganja na področju varnosti in odpornosti.

11.7 COBIT 2019:

11.7.1 BAI04 – Upravljanje razpoložljivosti in zmogljivosti: Zagotavlja, da so storitve v oblaku odporne, spremljane in izpolnjujejo določena merila uspešnosti.

11.7.2 DSS01 – Upravljanje operacij: Podpira operativno integracijo, obravnavo incidentov in izhodiščne konfiguracije na platformah, gostovanih v oblaku.

11.7.3 DSS05 – Upravljanje varnostnih storitev: Usmerja uvedbo varnostnih kontrol, spremljanje in preprečevanje incidentov, specifičnih za oblak, v digitalnih storitvah.