					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P27					Naziv dokumenta: **Politika korištenja usluga u oblaku**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Zahtjevi za operativno planiranje i kontrolu u okruženjima oblaka.
ISO/IEC 27002:2022	Kontrole 5.23–5.25	Zahtjevi za korištenje, politiku i sigurnost usluga u oblaku.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Korištenje vanjskih sustava, ugovorni i tehnički zahtjevi, kriptografska zaštita, sigurnost opskrbnog lanca.
EU GDPR	Članci 28, 32, Poglavlje V	Zahtjevi za izvršitelje obrade u oblaku, sigurnost obrade i prijenos podataka.
EU NIS2	Članak 21(2)(f, i)	Rizici trećih strana i zahtjevi povezani s opskrbnim lancem.
EU DORA	Članci 5(2), 28	Nadzor nad IKT-om i trećim stranama (oblak) za financijske subjekte.
COBIT 2019	BAI04, DSS01, DSS05	Dostupnost usluga u oblaku, operacije i upravljanje sigurnošću.

1. Svrha

1.1 Ova politika utvrđuje obvezne zahtjeve organizacije za sigurno, usklađeno i odgovorno korištenje usluga računalstva u oblaku u modelima isporuke Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) i Software-as-a-Service (SaaS).

1.2 Svrha ove politike jest osigurati da se usluge u oblaku uvode i njima upravlja na način koji štiti povjerljivost, cjelovitost i dostupnost informacijskih resursa, uz ispunjavanje regulatornih, zakonskih i ugovornih obveza.

1.3 Ova politika definira kontrole za upravljanje rizicima povezanima s oblakom, zaštitu podataka, praćenje usklađenosti pružatelja usluga te uklanjanje neovlaštenog korištenja. Također podupire poslovne inovacije putem platformi u oblaku usklađivanjem sigurnosti, operativne pouzdanosti i troškovne učinkovitosti.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve zaposlenike, ugovorne izvršitelje, pružatelje usluga trećih strana i vanjske konzultante koji u ime organizacije dodjeljuju, konfiguriraju, pristupaju, upravljaju ili koriste usluge u oblaku.

2.2 Primjenjuje se na sva okruženja u kojima se obrađuju podaci ili radna opterećenja organizacije, uključujući:

2.2.1 javne, privatne, hibridne i zajedničke modele oblaka

2.2.2 sve modele usluga u oblaku (IaaS, PaaS, SaaS)

2.2.3 višeoblačne i federirane arhitekture

2.2.4 korištenje shadow IT-a ili osobnih računa u oblaku u poslovne svrhe

2.3 Obuhvaća sve klasifikacijske razine podataka te se primjenjuje na interne sustave i platforme koje udomljuju dobavljači kada se na njima pohranjuju ili obrađuju podaci u vlasništvu organizacije ili regulirani podaci.

3. Ciljevi

3.1 Osigurati sigurno i dosljedno korištenje tehnologija u oblaku putem jasno definiranih pravila korištenja, sigurnosnih osnovica i upravljačkih uloga.

3.2 Smanjiti operativne i regulatorne rizike povezane s računalstvom u oblaku, uključujući neovlašteni pristup, povrede podataka, pogrešne konfiguracije, neusklađenost i prekide usluge.

3.3 Osigurati provedbu sigurnosnih i privatnosnih zahtjeva za sve dobavljače usluga u oblaku te provjeravati usklađenost putem ugovornih odredbi, procjena i prava na reviziju.

3.4 Omogućiti skalabilno i otporno uvođenje usluga u oblaku bez narušavanja sigurnosnog profila, zakonskih zahtjeva ili kontinuiteta poslovanja.

3.5 Uskladiti upravljanje korištenjem usluga u oblaku i njihovu uporabu s okvirom ISMS-a organizacije, zakonskim obvezama (npr. GDPR, DORA), sektorski specifičnim smjernicama i industrijski priznatim dobrim praksama (npr. NIST, COBIT).

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava Politiku korištenja usluga u oblaku i strateški plan uvođenja usluga u oblaku.

4.1.2 Preispituje i odobrava iznimke visokog rizika od standardnih zahtjeva za upravljanje uslugama u oblaku.

4.1.3 Osigurava da inicijative povezane s oblakom imaju odgovarajuće financiranje, nadzor i integraciju s okvirom upravljanja rizicima na razini organizacije.

4.2 Glavni direktor informacijske sigurnosti (CISO)

4.2.1 Vlasnik je ove politike i organizacijskog Registra usluga u oblaku.

4.2.2 Odobrava uvođenje novih pružatelja usluga u oblaku na temelju dubinske analize dobavljača i procjene rizika.

4.2.3 Preispituje dokumentaciju o usklađenosti pružatelja usluga i potvrđuje usklađenost sa sigurnosnim zahtjevima.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se preispitivati najmanje jednom godišnje i ažurirati prema potrebi kako bi ostala usklađena sa:

9.1.1 razvojem zakonskih i regulatornih zahtjeva (npr. GDPR, NIS2, DORA)

9.1.2 promjenama standarda ISO/IEC 27001 ili ISO/IEC 27002

9.1.3 ažuriranjima arhitekture oblaka, okruženja prijetnji ili portfelja usluga organizacije

9.1.4 istragama incidenata, rezultatima revizije ili naučenim lekcijama iz operativne uporabe

9.2 CISO je odgovoran za pokretanje pregleda i uključivanje relevantnih dionika, uključujući:

9.2.1 Arhitekta sigurnosti oblaka

9.2.2 tim za pravne poslove i usklađenost

9.2.3 nabavu i voditelje dobavljača

9.2.4 vlasnike usluga i IT operacije

9.3 Sva ažuriranja moraju biti:

9.3.1 pod verzijskom kontrolom i datirana

9.3.2 odobrena od strane Izvršnog rukovodstva

9.3.3 priopćena zahvaćenim stranama, uključujući zaposlenike, ugovorne izvršitelje i treće strane

9.3.4 arhivirana u skladu s internim politikama upravljanja dokumentacijom

9.4 Izvanredni pregledi mogu se pokrenuti zbog:

9.4.1 novih angažmana CSP-a ili većih migracija

9.4.2 novih prijetnji za infrastrukturu u oblaku

9.4.3 značajnih promjena u ugovornim, zakonskim ili sektorski specifičnim obvezama

10. Povezane politike i poveznice

10.1 Ova je politika usko povezana sa sljedećim internim politikama i o njima ovisi:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja krovna načela za siguran rad sustava i usluga, koja ova politika provodi u kontekstu oblaka.

10.1.2 P5 – Politika upravljanja promjenama: sve promjene konfiguracije u oblaku moraju slijediti postupke kontrole promjena utvrđene u P5.

10.1.3 P13 – Politika klasifikacije podataka i označavanja: određuje kako se podaci procjenjuju prije prijenosa u oblak i kako se primjenjuju kontrole kao što su šifriranje i rezidentnost podataka.

10.1.4 P18 – Politika kriptografskih kontrola: propisuje standarde za šifriranje, upravljanje ključevima i uporabu kriptografskih algoritama, koji se izravno primjenjuju u konfiguracijama usluga u oblaku.

10.1.5 P22 – Politika zapisivanja događaja i praćenja: propisuje zahtjeve za prikupljanje, čuvanje i analizu dnevničkih zapisa koji se moraju provoditi u okruženjima u oblaku.

10.1.6 P30 – Politika odgovora na incidente: definira postupke eskalacije, ograničavanja i sanacije za sigurnosne događaje povezane s oblakom.

10.1.7 P33 – Politika praćenja revizije i usklađenosti: podupire revizijsku spremnost i kontinuirano osiguranje da se kontrole u oblaku provode i nadziru.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001: Točka 8.1 – Operativno planiranje i kontrola: zahtijeva da organizacije uspostave i kontroliraju procese potrebne za ispunjavanje zahtjeva informacijske sigurnosti, uključujući one koji se odnose na okruženja u oblaku.

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

11.2.1 Dodatak A Kontrola 5.23 – Korištenje usluga u oblaku: zahtijeva procjenu temeljenu na riziku, formalno odobrenje i dokumentiranje korištenja usluga u oblaku.

11.2.2 Dodatak A Kontrola 5.24 – Politika korištenja usluga u oblaku: zahtijeva uspostavu i provedbu formalnih politika korištenja usluga u oblaku usklađenih s potrebama i rizicima organizacije.

11.2.3 Dodatak A Kontrola 5.25 – Sigurnost u uslugama u oblaku: zahtijeva integraciju sigurnosti, ugovornu zaštitu i praćenje radnih opterećenja i podataka smještenih u oblaku.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Korištenje vanjskih sustava: zahtijeva definirana pravila i uvjete za pristup resursima organizacije iz vanjskih sustava ili sustava u oblaku.

11.3.2 SA-9(5) – Usluge vanjskih informacijskih sustava: propisuje ugovorne sigurnosne zahtjeve, nadzor i kontinuirano praćenje za sustave u oblaku trećih strana.

11.3.3 SC-12 do SC-28 – Kriptografska zaštita, zaštita granica sustava i cjelovitost prijenosa: usklađeni su sa zahtjevima za šifriranje, identitet i pristup za usluge smještene u oblaku i podatke u prijenosu.

11.3.4 SR-5 – Sigurnost opskrbnog lanca: podupire provjeru i ugovornu kontrolu nad CSP-ovima uključenima u isporuku usluge.

11.4 GDPR EU (2016/679):

11.4.1 Članak 28 – Obveze izvršitelja obrade: zahtijeva formalne ugovore s pružateljima usluga u oblaku radi osiguranja sigurnosti, povjerljivosti i mogućnosti revizije obrade osobnih podataka.

11.4.2 Članak 32 – Sigurnost obrade: podupire primjenu šifriranja, kontrola pristupa, zapisivanja događaja i drugih zaštitnih mjera u okruženjima u oblaku.

11.4.3 Poglavlje V – Međunarodni prijenosi podataka: zahtijeva zakonit prijenos podataka izvan EU/EGP-a primjenom zaštitnih mjera kao što su SCC-ovi ili odluke o primjerenosti.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članak 21(2)(f, i): zahtijeva da subjekti upravljaju rizicima koje predstavljaju pružatelji usluga u oblaku trećih strana i osiguraju cjelovitost digitalnog opskrbnog lanca ugovornim i tehničkim mjerama.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Članak 5(2) – Upravljanje IKT rizicima: zahtijeva integraciju rizika trećih strana povezanih s IKT-om, uključujući usluge u oblaku, u cjelokupno upravljanje rizicima.

11.6.2 Članak 28 – Nadzor nad kritičnim IKT pružateljima usluga trećih strana: zahtijeva da financijski subjekti prate, kontroliraju i izvješćuju o ovisnostima o pružateljima usluga u oblaku, njihovu sigurnosnom profilu i otpornosti.

11.7 COBIT 2019:

11.7.1 BAI04 – Upravljanje dostupnošću i kapacitetom: osigurava da su usluge u oblaku otporne, da se nadziru i da ispunjavaju definirane kriterije učinkovitosti.

11.7.2 DSS01 – Upravljanje operacijama: podupire operativnu integraciju, postupanje s incidentima i osnovne konfiguracije na platformama smještenima u oblaku.

11.7.3 DSS05 – Upravljanje sigurnosnim uslugama: usmjerava provedbu sigurnosnih kontrola specifičnih za oblak, praćenje i sprječavanje incidenata u digitalnim uslugama.