					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P27S					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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	
ISO/IEC 27002:2022	Kontrole 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
GDPR EU	Članak 28, 32 i poglavlje V	
Direktiva EU NIS2	Članci 21(2)(f), (i)	
Uredba EU DORA	Članci 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI	

1. Svrha

1.1 Ova politika definira kako se usluge u oblaku smiju sigurno koristiti unutar organizacije. Njome se osigurava zaštita podataka koji se obrađuju ili pohranjuju u oblaku, uspostava kontrole pristupa te odgovorno upravljanje rizicima.

1.2 Ova politika pomaže malim i srednjim poduzećima u ispunjavanju zakonskih obveza i očekivanja klijenata u pogledu zaštite osjetljivih informacija, sprječavanja curenja podataka i učinkovitog upravljanja rizicima povezanima s uslugama u oblaku, bez potrebe za infrastrukturom na razini velikih poduzeća.

1.3 Ova politika podupire certifikaciju prema normi ISO/IEC 27001, usklađenost s GDPR-om i sigurnost opskrbnog lanca kroz dosljedno upravljanje svim uslugama u oblaku koje pružaju treće strane.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 svaku uslugu u oblaku koja se koristi za pohranu, obradu ili prijenos podataka organizacije

2.1.2 sve zaposlenike, ugovorne izvođače i pružatelje usluga koji u ime organizacije koriste alate u oblaku

2.1.3 besplatna i komercijalna rješenja u oblaku, uključujući platforme e-pošte, dijeljenje dokumenata, SaaS alate, platforme za sigurnosne kopije, alate za videokonferencije i platforme za rad s klijentima

2.1.4 svaki uređaj (stolno računalo, mobilni uređaj, tablet) koji putem aplikacija u oblaku pristupa informacijama organizacije

2.2 To uključuje, ali nije ograničeno na:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 alate u oblaku za sigurnosno kopiranje i oporavak od katastrofe

2.2.5 zajedničke mape ili aplikacije koje se koriste za izdavanje računa, upravljanje projektima ili komunikaciju s klijentima

3. Ciljevi

3.1 Spriječiti neovlašteno korištenje neodobrenih usluga u oblaku ili njihovo korištenje koje predstavlja visok rizik.

3.2 Osigurati da su osjetljivi ili regulirani podaci pohranjeni u oblaku zaštićeni odgovarajućim tehničkim i organizacijskim kontrolama.

3.3 Utvrditi jasne uloge za odobravanje, konfiguriranje, nadzor i stavljanje izvan uporabe usluga u oblaku.

3.4 Kontrolirati tokove podataka te osigurati provedbu obveza čuvanja, brisanja i privatnosti za informacije pohranjene u oblaku.

3.5 Smanjiti oslanjanje na osobne račune ili neevidentirane alate zahtijevanjem odobrenja za sve sustave u oblaku koji se koriste u poslovne svrhe.

3.6 Osigurati usklađenost sa zahtjevima norme ISO/IEC 27001:2022, GDPR-a, NIS2 i DORA-e u pogledu upravljanja vanjskim ovisnostima o uslugama u oblaku.

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 odobrava korištenje svih novih usluga u oblaku

4.1.2 preispituje rizike povezane s pružateljima usluga u oblaku i vrstama usluga

4.1.3 osigurava primjenu ove politike i nadzire odluke o iznimkama

4.2 pružatelj IT podrške ili tehnička podrška

4.2.1 procjenjuje i uvodi sigurnu konfiguraciju za usluge u oblaku

4.2.2 uspostavlja račune, kontrolu pristupa i sigurnosne kopije

4.2.3 prati usklađenost s pravilima za lozinke, višefaktorskom autentifikacijom (MFA) i sigurnosnim postavkama

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku moraju najmanje jednom godišnje pregledati glavni direktor, u koordinaciji s pružateljem IT podrške.

9.2 Formalni pregled mora se provesti i u sljedećim slučajevima:

9.2.1 nakon sigurnosnog incidenta povezanog s oblakom (npr. povreda sigurnosti, gubitak podataka)

9.2.2 kada se uvodi nova glavna platforma u oblaku

9.2.3 ako se promijene zakonski ili regulatorni zahtjevi (npr. ažuriranja GDPR-a, NIS2 ili DORA-e)

9.2.4 ako aktivnosti praćenja otkriju zlouporabu ili nove rizike

9.3 Glavni direktor mora osigurati:

9.3.1 da se Registar usluga u oblaku ažurira novim uslugama ili uslugama stavljenima izvan uporabe

9.3.2 da su pravni zahtjevi i zahtjevi zaštite privatnosti i dalje ispunjeni

9.3.3 da se sve promjene priopće relevantnim korisnicima i dionicima

9.4 Arhivirane verzije moraju se sigurno pohranjivati, a sa starim verzijama politike mora se postupati u skladu s politikom organizacije P14S – Politika zadržavanja i zbrinjavanja podataka.

10. Povezane politike i poveznice

10.1 Ova politika mora se primjenjivati zajedno sa sljedećim SME politikama informacijske sigurnosti:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: definira odgovornost za odobravanje usluga u oblaku i upravljanje odnosima s pružateljima usluga.

10.1.2 P4S – Politika kontrole pristupa: podupire sigurnu prijavu, upravljanje sesijama i prakse ukidanja prava pristupa potrebne za platforme u oblaku.

10.1.3 P14S – Politika zadržavanja i zbrinjavanja podataka: uređuje kako se podaci u oblaku sigurnosno kopiraju, čuvaju i brišu u skladu sa zakonskim obvezama.

10.1.4 P17S – Politika zaštite podataka i privatnosti: osigurava da se sa svim osobnim podacima pohranjenima u uslugama u oblaku postupa u skladu s načelima GDPR-a.

10.1.5 P30S – Politika odgovora na incidente: utvrđuje strukturirane postupke za odgovor na sigurnosne incidente povezane s oblakom, uključujući prikupljanje dokaza i vanjsko obavješćivanje.

10.2 Zajedno, ove politike osiguravaju da je korištenje oblaka sigurno, usklađeno i operativno otporno.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – zahtijeva da organizacije uspostave operativne kontrole za postupanje s podacima, uključujući kontrole povezane sa sustavima u oblaku.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.23 – zahtijeva upravljanje korištenjem usluga u oblaku i SaaS alata trećih strana.

11.2.2 Kontrola 5.24 – zahtijeva definiranu politiku korištenja oblaka usklađenu s rizicima i regulatornim zahtjevima.

11.2.3 Kontrola 5.25 – zahtijeva da organizacije osiguraju da sigurnosne kontrole u okruženjima u oblaku odgovaraju potrebama organizacije.

11.3 NIST SP 800-53 Rev.

11.3.1 AC-20 – zahtijeva formalne politike korištenja za vanjske sustave kao što su usluge u oblaku.

11.3.2 SC-12, SC-13 – odnose se na šifriranje podataka u prijenosu i podataka u mirovanju u okruženjima u oblaku.

11.3.3 SR-5 – obuhvaća kontrole rizika za oblak i treće strane unutar opskrbnog lanca.

11.4 GDPR EU (2016/679)

11.4.1 Članak 28 – zahtijeva da pružatelji usluga u oblaku koji djeluju kao izvršitelji obrade postupaju u skladu s obvezujućim ugovornim obvezama.

11.4.2 Članak 32 – zahtijeva tehničke i organizacijske kontrole za obradu podataka u oblaku.

11.4.3 Poglavlje V – zabranjuje neovlaštene međunarodne prijenose osobnih podataka pohranjenih u oblaku.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(f), (i) – zahtijeva da ključni i važni subjekti uspostave odgovarajuće politike za sigurnost usluga u oblaku i kontrolu opskrbnog lanca.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 5(2) – zahtijeva da financijski SME subjekti integriraju sigurnost oblaka u svoje okvire za upravljanje IKT rizicima.

11.6.2 Članak 28 – uspostavlja pravila nadzora nad kritičnim pružateljima IKT usluga trećih strana, uključujući pružatelje usluga u oblaku.

11.7 COBIT 2019

11.7.1 DSS01 – „Upravljanje operacijama” odnosi se na operativni integritet usluga u oblaku.

11.7.2 DSS05 – „Upravljanje sigurnosnim uslugama” uključuje zaštitne mjere i praćenje specifično za oblak.

11.7.3 BAI04 – „Upravljanje dostupnošću i kapacitetom” osigurava kontinuitet poslovanja i performanse u okruženjima u oblaku.