					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P26S					Naziv dokumenta: **Politika sigurnosti trećih strana i dobavljača**							
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	Operativne kontrole za odnose s trećim stranama i dobavljačima
ISO/IEC 27002:2022	Kontrole 5.19–5.22	Kontrole sigurnosti dobavljača, ugovorne sigurnosne odredbe, upravljanje promjenama te praćenje i pregled
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Nabava, konfiguracija, sporazumi o međupovezivanju i kontrole za vanjsko osoblje
GDPR EU	Članci 28, 32	ugovor o obradi podataka, sigurnosni zahtjevi za izvršitelje obrade
Direktiva EU NIS2	Članci 21(2)(a)(b)(i), 23(1)	upravljanje rizicima opskrbnog lanca, nadzor nad uslugama trećih strana
Uredba EU DORA	Članci 5(1)(2), 28(1)(2)	upravljanje IKT rizicima za pružatelje usluga trećih strana
COBIT 2019	APO10, APO12, DSS05	upravljanje dobavljačima i integracija rizika

1. Svrha

1.1 Ova politika utvrđuje obvezne sigurnosne zahtjeve za uspostavu, upravljanje i prestanak odnosa s trećim stranama i dobavljačima koji pristupaju podacima, sustavima ili uslugama organizacije ili na njih utječu.

1.2 Ovom se politikom osigurava da vanjski pružatelji usluga, uključujući pružatelje IT podrške, operatore usluga u oblaku, inženjere razvoja softvera i ugovorne izvođače poslovnih procesa, postupaju s imovinom organizacije na siguran način i u skladu s primjenjivim zakonima i standardima.

1.3 Ova politika smanjuje rizike kao što su curenje podataka, neovlaštene izmjene sustava, regulatorne kazne ili prekidi poslovanja uzrokovani nesigurnim ili nedostatno uređenim aranžmanima s trećim stranama.

2. Opseg

2.1 Ova politika primjenjuje se na sve treće strane koje:

2.1.1 pružaju softver, infrastrukturu, usluge hostinga ili usluge u oblaku

2.1.2 pristupaju internim sustavima, uređajima ili aplikacijama ili njima upravljaju

2.1.3 obrađuju podatke organizacije, dokumente ili sigurnosne kopije

2.1.4 podržavaju poslovne operacije, ljudske resurse (HR), financije ili korisničke usluge

2.2 Ova politika također se primjenjuje na:

2.2.1 interno osoblje uključeno u odabir, angažiranje ili nadzor dobavljača

2.2.2 svako osoblje koje upravlja uvođenjem dobavljača, ugovorima, pristupom ili pregledima

2.2.3 svaki sustav ili proces koji ovisi o komponentama ili uslugama trećih strana

3. Ciljevi

3.1 Osigurati da svi dobavljači ispunjavaju jasno definirane sigurnosne zahtjeve.

3.2 Zahtijevati da ugovori s dobavljačima uključuju provedive obveze u području sigurnosti, privatnosti i odgovora na incidente.

3.3 Procijeniti i dokumentirati rizike povezane s dobavljačima prije sklapanja ugovora ili dodjele pristupa.

3.4 Provoditi redovite preglede visokorizičnih ili kritičnih dobavljača radi potvrde usklađenosti.

3.5 Uspostaviti formalan postupak za iznimke, upravljanje incidentima i ažuriranje ugovora.

3.6 Podržati usklađenost s obvezama iz normi ISO/IEC 27001:2022, GDPR-a, NIS2 i DORA-e koje se odnose na upravljanje dobavljačima.

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 snosi krajnju odgovornost za odabir dobavljača i usklađenost sa sigurnosnim zahtjevima

4.1.2 odobrava ugovore, iznimke i eskalacije koje uključuju dobavljače

4.1.3 nadzire odgovor na incidente i donošenje odluka kada dobavljači ne ispune svoje obveze

4.2 pružatelj IT podrške ili interni kontakt za informacijsku sigurnost

4.2.1 procjenjuje tehnički pristup koji dobavljači zahtijevaju

4.2.2 provodi pravila kontrole pristupa, pregledava dnevničke zapise i potvrđuje sigurno postupanje s podacima

4.2.3 pregledava dokaze o sigurnosnim kontrolama, sigurnosnim certifikatima ili nalazima revizije, gdje je primjenjivo

[... 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 mora pregledati najmanje jednom godišnje glavni direktor, uz sudjelovanje pružatelja IT podrške ili voditelja dobavljača.

9.2 Politika se također mora pregledati:

9.2.1 nakon svake značajne promjene zakonskih, regulatornih ili ugovornih obveza

9.2.2 nakon sigurnosnog incidenta povezanog s dobavljačem ili nalaza revizije

9.2.3 pri uvođenju novih kategorija dobavljača, primjerice kritičnih SaaS platformi

9.3 Sva ažuriranja moraju biti:

9.3.1 dokumentirana s poviješću verzija i obrazloženjem

9.3.2 odobrena od strane glavnog direktora

9.3.3 priopćena relevantnom internom osoblju i voditeljima dobavljača

9.3.4 pohranjena zajedno s prethodnim verzijama u skladu s P14S – Politikom zadržavanja i zbrinjavanja podataka

10. Povezane politike i poveznice

10.1 Djelotvornost ove politike ovisi o usklađenom djelovanju sa sljedećim SME politikama informacijske sigurnosti:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje odgovornost za nadzor nad dobavljačima i provedbu ugovornih obveza.

10.1.2 P4S – Politika kontrole pristupa: propisuje pravila ograničavanja pristupa koja se moraju primijeniti kada se dobavljačima dodjeljuje pristup sustavu.

10.1.3 P17S – Politika zaštite podataka i privatnosti: osigurava da dobavljači koji obrađuju osobne podatke poštuju načela zaštite podataka i zakonske zahtjeve.

10.1.4 P14S – Politika zadržavanja i zbrinjavanja podataka: primjenjuje se na sve podatke ili zapise koji se dijele s dobavljačima ili ih dobavljači pohranjuju te uređuje sigurno zbrinjavanje nakon prestanka ugovora.

10.1.5 P30S – Politika odgovora na incidente: definira način postupanja kada dobavljač uzrokuje sigurnosni incident ili je u njega uključen, uključujući eskalaciju i postupke rukovanja dokazima.

10.2 Ove politike zajedno osiguravaju da se rizik povezan s dobavljačima drži pod kontrolom tijekom cijelog životnog ciklusa ugovora.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – zahtijeva provedbu operativnih kontrola, uključujući one koje se primjenjuju na odnose s trećim stranama i dobavljačima.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.19 – osigurava da su sigurnosne mjere dobavljača usklađene sa zahtjevima organizacije.

11.2.2 Kontrola 5.20 – zahtijeva formalne ugovore koji obuhvaćaju sigurnosne odredbe, odgovornosti i obveze u slučaju povrede.

11.2.3 Kontrola 5.21 – uređuje promjene u uslugama dobavljača koje mogu utjecati na sigurnosni profil.

11.2.4 Kontrola 5.22 – zahtijeva praćenje i pregled usluga dobavljača i usklađenosti.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – uređuje nabavu vanjskih sustava i usluga te zahtijeva procjene rizika i jasno definirana očekivanja.

11.3.2 SA-10 – uređuje konfiguraciju i postupke promjena koji uključuju sustave kojima upravljaju treće strane.

11.3.3 CA-3 – zahtijeva sporazume o međupovezivanju za sustave koji uključuju vanjske subjekte.

11.3.4 PS-7 – propisuje provjeru i odgovornost za vanjsko osoblje.

11.4 GDPR EU (2016/679)

11.4.1 Članak 28 – zahtijeva ugovor o obradi podataka s dobavljačima koji djeluju kao izvršitelji obrade.

11.4.2 Članak 32 – propisuje odgovarajuće tehničke i organizacijske sigurnosne mjere za sve izvršitelje obrade.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(a), (b), (i) – propisuje upravljanje rizicima IKT opskrbnog lanca i kontrole za treće strane.

11.5.2 Članak 23(1) – zahtijeva dokumentiran nadzor nad uslugama trećih strana za ključne i važne subjekte.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 5(1) – zahtijeva okvir za upravljanje IKT rizicima koji obuhvaća sve kritične pružatelje usluga trećih strana.

11.6.2 Članak 5(2) – propisuje ugovorne i operativne kontrole za ovisnosti o IKT uslugama.

11.6.3 Članak 28(1), (2) – uspostavlja pravila nadzora nad IKT rizikom trećih strana u financijskom sektoru.

11.7 COBIT 2019

11.7.1 APO10 – „Upravljanje dobavljačima” opisuje kontrole nabave i očekivanja u upravljanju odnosima.

11.7.2 APO12 – „Upravljanje rizicima” integrira rizik dobavljača u upravljanje organizacijskim rizicima.

11.7.3 DSS05 – „Upravljanje sigurnosnim uslugama” primjenjuje se na pružatelje upravljanih usluga i vanjski ugovorene pružatelje usluga trećih strana.