					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P26					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 propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Operativno planiranje i kontrola: zahtijeva formalne kontrole nad uslugama trećih strana koje utječu na ISMS
ISO/IEC 27002:2022	Kontrole 5.19–5.22	Politike i postupci za odnose s dobavljačima; upravljanje rizicima dobavljača; upravljanje isporukom usluga dobavljača; praćenje i preispitivanje dobavljača
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Usluge vanjskih sustava; upravljanje konfiguracijom razvojnih inženjera; međupovezivanje sustava; sigurnost osoblja trećih strana
GDPR EU	Članci 28, 32, 33	Obveze izvršitelja obrade, sigurnost obrade, obavješćivanje o povredi osobnih podataka
Direktiva EU NIS2	Članak 21(2)(e–f)	upravljanje dobavljačima temeljeno na riziku i sigurnosni nadzor
Uredba EU DORA	Članci 28, 30	rizik IKT trećih strana, nadzor nad kritičnim pružateljima IKT usluga trećih strana
COBIT 2019	BAI05, DSS02, MEA03	Upravljanje omogućavanjem organizacijskih promjena; upravljanje zahtjevima za uslugama i incidentima; praćenje, vrednovanje i procjena usklađenosti

1. Svrha

1.1 Ova politika definira zahtjeve informacijske sigurnosti za uspostavu, upravljanje i održavanje sigurnih odnosa s dobavljačima i pružateljima usluga trećih strana.

1.2 Njome se osigurava da svi dobavljači koji imaju pristup podacima, sustavima ili infrastrukturi organizacije podliježu strogim sigurnosnim kontrolama, ugovornim zaštitnim mjerama i kontinuiranom nadzoru tijekom cijelog životnog ciklusa usluge.

1.3 Ova politika podupire kontrole 5.19 do 5.22 iz Priloga A norme ISO/IEC 27001 uključivanjem sigurnosnih zahtjeva u postupak nabave, uvođenje dobavljača, dubinsku analizu dobavljača, upravljanje ugovorima, praćenje usluga i postupke prestanka suradnje.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 sve dobavljače, ugovorne izvođače, pružatelje usluga u oblaku i uslužne organizacije trećih strana koji obrađuju ili kojima je omogućen pristup informacijskim resursima organizacije

2.1.2 sve interne uloge uključene u procjenu dobavljača, uvođenje dobavljača, ugovaranje, upravljanje rizicima, praćenje ili prestanak suradnje

2.1.3 sve odnose s dobavljačima koji uključuju pristup osjetljivim podacima, integraciju s produkcijskim uslugama ili podršku kritičnim poslovnim funkcijama

2.2 Politika obuhvaća i izravne dobavljače i njihove podizvršitelje obrade, kada je primjenjivo, te uključuje softver trećih strana, infrastrukturu, podršku i pružatelje upravljanih usluga.

3. Ciljevi

3.1 Osigurati da se sigurnosni rizici povezani s dobavljačima dosljedno identificiraju, procjenjuju i ublažavaju tijekom cijelog životnog ciklusa odnosa.

3.2 Uključiti standardizirane sigurnosne zahtjeve u sve ugovore s dobavljačima, uključujući obveze obavješćivanja o povredi, prava na reviziju i odgovornosti za zaštitu podataka.

3.3 Zahtijevati formalnu dubinsku analizu dobavljača i dokumentirane procjene rizika prije angažiranja novih dobavljača ili obnove ugovora o uslugama visokog rizika.

3.4 Uspostaviti mehanizme za kontinuirano praćenje usklađenosti dobavljača, uključujući preglede uspješnosti, revizije i eskalaciju incidenata.

3.5 Upravljati promjenama usluga dobavljača te osigurati siguran izlazni proces i povrat ili uništenje podataka pri prestanku suradnje.

3.6 Uskladiti sigurnosne kontrole trećih strana s primjenjivim regulatornim i ugovornim obvezama, uključujući GDPR, NIS2, DORA i standarde ISO/IEC 27001.

4. Uloge i odgovornosti

4.1 glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu usklađenost s cjelokupnim ISMS-om, upravljanjem rizicima i strategijom usklađenosti.

4.1.2 Odobrava razine klasifikacije dobavljača, ishode sigurnosnih pregleda i iznimke visokog rizika.

4.1.3 Sudjeluje u eskalaciji ozbiljnih incidenata povezanih s dobavljačima i u pregovorima o ugovorima za kritične usluge.

4.2 Nabava i upravljanje dobavljačima

4.2.1 Osigurava da svi novi i obnovljeni ugovori s dobavljačima uključuju odobrene odredbe o sigurnosti i zaštiti podataka.

4.2.2 Održava središnji registar dobavljača i koordinira s funkcijama ljudskih resursa, pravnih poslova i usklađenosti dokumentaciju o rizicima trećih strana.

4.2.3 Pokreće procese uvođenja dobavljača i osigurava usklađenost s procjenama sigurnosti prije sklapanja ugovora.

[... 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 ili ranije u slučaju:

9.1.1 značajnih promjena strategije nabave ili ekosustava dobavljača

9.1.2 ažuriranja pravnog ili regulatornog okvira (npr. DORA, GDPR)

9.1.3 većih incidenata trećih strana, povreda podataka ili neuspjeha na reviziji

9.1.4 nalaza procjena rizika ili vanjskih certifikacijskih tijela

9.2 Za postupak preispitivanja zajednički su odgovorni CISO, nabava, pravni poslovi i funkcija upravljanja rizicima.

9.3 Sve izmjene politike moraju biti dokumentirane u registru upravljanja dokumentima ISMS-a, pod verzijskom kontrolom i priopćene relevantnim dionicima putem kanala upravljanja dobavljačima i programa podizanja svijesti zaposlenika.

9.4 Verzije koje više nisu na snazi moraju se arhivirati najmanje tri godine radi sljedivosti i pravne usklađenosti.

10. Povezane politike i poveznice

10.1 P1 – Politika informacijske sigurnosti. Utvrđuje krovnu obvezu sigurnog provođenja svih operacija organizacije, uključujući oslanjanje na dobavljače trećih strana i vanjske pružatelje usluga.

10.2 P6 – Politika upravljanja rizicima. Usmjerava identifikaciju, procjenu i ublažavanje rizika povezanih s odnosima s trećim stranama, uključujući naslijeđene ili sistemske rizike iz ekosustava dobavljača.

10.3 P17 – Politika zaštite podataka i privatnosti. Primjenjuje se na sve dobavljače koji postupaju s osobnim podacima te zahtijeva odgovarajuće ugovorne uvjete, zaštitne mjere za prijenos i načela ugrađene privatnosti.

10.4 P4 – Politika kontrole pristupa. Uređuje način na koji osoblje trećih strana dobiva pristup sustavima organizacije, uz primjenu ovlaštenja temeljenih na ulogama, kontrola sesija i postupaka ukidanja prava pristupa.

10.5 P22 – Politika zapisivanja događaja i praćenja. Zahtijeva da se pristup sustavima od strane dobavljača prati, evidentira i preispituje, osobito u okruženjima u kojima se provode privilegirane aktivnosti ili aktivnosti usmjerene na podatke.

10.6 P30 – Politika odgovora na incidente. Definira postupke eskalacije i zahtjeve za prijavu povreda za sigurnosne događaje koji potječu od dobavljača ili za zajedničke istrage koje uključuju sustave trećih strana.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001: Točka 8.1 – Operativno planiranje i kontrola: zahtijeva formalne kontrole nad uslugama trećih strana koje utječu na ISMS.

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

11.2.1 Kontrola 5.19 iz Priloga A – Politike i postupci za odnose s dobavljačima: nalaže kontrole za upravljanje interakcijama s dobavljačima.

11.2.2 Kontrola 5.20 iz Priloga A – Upravljanje rizicima dobavljača: usmjerena je na identifikaciju, procjenu i kontinuirani nadzor sigurnosnog profila dobavljača.

11.2.3 Kontrola 5.21 iz Priloga A – Upravljanje isporukom usluga dobavljača: zahtijeva usklađenost uspješnosti i sigurnosti s ugovornim očekivanjima.

11.2.4 Kontrola 5.22 iz Priloga A – Praćenje i preispitivanje dobavljača: naglašava potrebu za kontinuiranom provjerom i ponovnom procjenom usklađenosti trećih strana.

11.3 NIST SP 800-53 Rev.:

11.3.1 SA-9 – Usluge vanjskih sustava: definira sigurnosne zahtjeve i zahtjeve za upravljanje rizikom za sustave kojima upravljaju vanjski subjekti.

11.3.2 SA-10 – Upravljanje konfiguracijom razvojnih inženjera: primjenjuje se kada treće strane isporučuju softver ili okruženja.

11.3.3 CA-3 – Međupovezivanje sustava: zahtijeva nadzor i dogovor o tokovima podataka između sustava različitih subjekata.

11.3.4 PS-7 – Sigurnost osoblja trećih strana: osigurava da se ugovorni izvođači i osoblje dobavljača primjereno provjeravaju i nadziru.

11.4 GDPR EU (2016/679):

11.4.1 Članak 28 – Obveze izvršitelja obrade: zahtijeva pisane ugovore s izvršiteljima obrade, uključujući tehničke i organizacijske mjere (TOM).

11.4.2 Članak 32 – Sigurnost obrade: nalaže odgovarajuće zaštitne mjere i za voditelje obrade i za izvršitelje obrade.

11.4.3 Članak 33 – Obavješćivanje o povredi osobnih podataka: zahtijeva žurno obavješćivanje dobavljača u slučaju povrede.

11.5 Direktiva NIS2 EU (2022/2555):

11.5.1 Članak 21(2)(e–f): zahtijeva upravljanje dobavljačima temeljeno na riziku i sigurnosni nadzor, osobito u digitalnim opskrbnim lancima ključnih i važnih subjekata.

11.6 Uredba DORA EU (2022/2554):

11.6.1 Članak 28 – Rizik IKT trećih strana: propisuje obveze procjene rizika, ugovornih sigurnosnih uvjeta i izlaznih strategija za pružatelje financijskih usluga.

11.6.2 Članak 30 – Nadzor nad kritičnim pružateljima IKT usluga trećih strana: uspostavlja pojačano praćenje i nadzorna očekivanja za ključne dobavljače.

11.7 COBIT 2019:

11.7.1 BAI05 – Upravljanje omogućavanjem organizacijskih promjena: osigurava da se prijelazi povezani s dobavljačima provode uz sigurno upravljanje.

11.7.2 DSS02 – Upravljanje zahtjevima za uslugama i incidentima: primjenjuje se na probleme koje prijavljuju dobavljači i na integraciju postupanja s incidentima.

11.7.3 MEA03 – Praćenje, vrednovanje i procjena usklađenosti: dodatno naglašava mjerenje uspješnosti dobavljača i praćenje usklađenosti.