					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P41					Naziv dokumenta: **Politika upravljanja rizikom ovisnosti o dobavljačima**							
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/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	6.1.3, 8.1, 9.1	
ISO/IEC 27002:2022	5.20, 5.21, 5.22, 5.23, 5.30	
NIST SP 800-53 Rev.5	SR-2, SR-3, SR-5, SR-6, SR-11, RA-3	
GDPR EU	čl. 28, čl. 32. st. 1. t. (d)	
Direktiva EU NIS2	čl. 21. st. 2. t. (d), čl. 21. st. 3., čl. 22.	
Uredba EU DORA	čl. 28.–30.	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Svrha

1.1 Ovom politikom unapređuju se prakse sigurnosti opskrbnog lanca organizacije uspostavom postupka za prepoznavanje i upravljanje kritičnim ovisnostima o dobavljačima i pružateljima usluga, u skladu sa zahtjevima iz članka 21. stavka 3. Direktive NIS2 i procjenama rizika opskrbnog lanca na razini Unije.

1.2 Ovom politikom osigurava se da se rizici koji proizlaze iz koncentracije ili oslanjanja na pojedinačne dobavljače razumiju i ublažavaju te da se svi sektorski specifični rizici opskrbnog lanca, na koje nadležna tijela upozoravaju u skladu s člankom 22. Direktive NIS2, uključe u naš program upravljanja rizicima i planiranje neprekidnosti poslovanja.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve ključne dobavljače i pružatelje usluga na koje se organizacija oslanja za kritične operacije, osobito one u IKT opskrbnom lancu (hardver, softver, usluge u oblaku, telekomunikacije, upravljane usluge).

2.2 Obuhvaća interne funkcije, uključujući nabavu, upravljanje dobavljačima, upravljanje rizicima i relevantne operativne odjele. Također obuhvaća i same dobavljače u mjeri potrebnoj za prikupljanje informacija o riziku. „Kritični dobavljači" su oni čiji bi neuspjeh ili kompromitacija mogli značajno utjecati na našu sposobnost pružanja usluga ili ispunjavanja zakonskih obveza.

3. Ciljevi

3.1 Osigurati pregled ovisnosti u opskrbnom lancu, osobito prepoznavanjem pojedinačnih točaka otkaza ili visokog rizika koncentracije u bazi dobavljača (npr. ovisnost o jednom pružatelju usluga u oblaku za sve usluge).

3.2 Uspostaviti mjere za smanjenje i upravljanje rizicima povezanima s dobavljačima, kao što su diversifikacija, planovi neprekidnosti poslovanja ili zahtijevanje pojačanih kontrola kod dobavljača, čime se povećava otpornost na neuspjehe dobavljača ili napade koji potječu iz opskrbnog lanca.

3.3 Uskladiti se sa zahtjevima Direktive NIS2 uključivanjem rezultata svih koordiniranih procjena sigurnosnih rizika kritičnih opskrbnih lanaca, u skladu s člankom 22., u organizacijsko odlučivanje o rizicima te osigurati da je naš pristup rizicima opskrbnog lanca dokumentiran i dokaziv.

4. Uloge i odgovornosti

4.1 Ured za upravljanje dobavljačima (VMO): vodi registar ovisnosti o dobavljačima i koordinira procjene rizika. Osigurava da se tijekom uvođenja dobavljača i periodično nakon toga svaki ključni dobavljač procijeni prema kritičnosti i razini ovisnosti.

4.2 Funkcija upravljanja rizicima (odbor za rizike organizacije): preispituje rizik koncentracije i analize ovisnosti, potvrđuje strategije obrade rizika (npr. odobrava uključivanje alternativnog dobavljača ili održavanje dodatnih zaliha kritičnih komponenti). Uključuje rizike opskrbnog lanca u registar rizika organizacije i izvješćuje najviše rukovodstvo.

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

9. Praćenje i revizija

9.1 Registar ovisnosti i procjene rizika podliježu godišnjoj unutarnjoj reviziji. Tim unutarnje revizije provjerava jesu li svi kritični dobavljači evidentirani, jesu li njihove ocjene rizika ažurne te jesu li planovi ublažavanja uspostavljeni i provode li se. Također provjerava jesu li vanjski ulazni podaci za procjenu rizika (izvješća iz članka 22. i slično) uredno uzeti u obzir.

9.2 Djelotvornost mjera diversifikacije i neprekidnosti poslovanja mora se periodično testirati. Primjerice, može se provesti planirana simulacija u kojoj se pretpostavlja neuspjeh važnog dobavljača kako bi se testirali naši planovi neprekidnosti poslovanja i alternativna rješenja (slično vježbi oporavka od katastrofe, ali za prekid usluge dobavljača). Rezultati tih testova moraju se dokumentirati, a svi nedostaci otkloniti.

9.3 Metrike: funkcija upravljanja rizicima prati metrike kao što su „% kritičnih usluga za koje je dostupan najmanje jedan alternativni dobavljač ili rješenje” ili „Top 5 ovisnosti o dobavljačima i njihov trend rizika”. Te metrike uključuju se u nadzorne ploče rizika za rukovodstvo. Silazni trend rizika ovisnosti tijekom vremena predstavlja cilj; ako metrike pokažu rastuću ovisnost, to mora potaknuti raspravu na razini uprave.

10. Pregled i održavanje

10.1 Ovu politiku najmanje jednom godišnje preispituju timovi za upravljanje dobavljačima i upravljanje rizicima. Preispitivanje uključuje sve promjene u okruženju dobavljača (npr. ako novi dobavljač postane kritičan ili se stari postupno isključi) te sve nove regulatorne zahtjeve za izdvojene usluge ili rizik trećih strana.

10.2 Ako sektorska tijela izdaju ažurirane smjernice ili incident pokaže nedostatke u kontrolama (primjerice, ako je prekid usluge dobavljača imao veći utjecaj od očekivanog, što upućuje na to da je procjena rizika pogrešno ocijenila razinu ovisnosti), politika će se ažurirati radi dorade kriterija ili strategija ublažavanja.

10.3 Revidirane verzije politike mora odobriti više rukovodstvo. Značajne promjene priopćit će se svim relevantnim odjelima, a materijali za osposobljavanje ažurirat će se u skladu s tim kako bi odražavali nove postupke ili standarde.

11. Povezane politike i poveznice

11.1 P01 – Politika informacijske sigurnosti. Dodjeljuje odgovornost za upravljanje ovisnostima o dobavljačima.

11.2 P02 – Politika uloga i odgovornosti u upravljanju. Pojašnjava vlasništvo nad odlukama o riziku povezanom s dobavljačima.

11.3 P06 – Politika upravljanja rizicima. Uključuje rizik koncentracije u registre rizika organizacije.

11.4 P26 – Politika sigurnosti trećih strana i dobavljača. Utvrđuje osnovnu razinu sigurnosti; P41 dodaje kontrole ovisnosti i koncentracije.

11.5 P27 – Politika korištenja usluga u oblaku. Primjenjuje kriterije ovisnosti na uvođenje usluga u oblaku i planove izlaska.

11.6 P28 – Politika razvoja s vanjskim izvršiteljima. Obuhvaća rizike ovisnosti u vanjskom razvoju i inženjeringu.

11.7 P32 – Politika neprekidnosti poslovanja i oporavka od katastrofe. Obuhvaća scenarije prekida usluge dobavljača i zamjene dobavljača.

11.8 P37 – Politika pravne i regulatorne usklađenosti. Osigurava da ugovori i obveze odražavaju kontrole ovisnosti.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), članak 21. stavak 3. (zahtijeva uzimanje u obzir ranjivosti specifičnih za svakog izravnog dobavljača/pružatelja usluga i kvalitete njihove kibernetičke sigurnosti, uključujući rezultate koordiniranih procjena rizika opskrbnog lanca)

12.2 Direktiva NIS2, članak 22. stavak 1. (koordinirane procjene sigurnosnih rizika kritičnih opskrbnih lanaca na razini Unije – informiraju subjekte o sektorskim rizicima povezanima s dobavljačima)

12.3 Provedbena uredba Komisije (EU) 2024/2690, Prilog, odjeljak 5. (zahtjevi sigurnosti opskrbnog lanca za subjekte, uključujući kriterije za odabir dobavljača, diversifikaciju i ugovorne obveze)

12.4 Dobre prakse ENISA-e za kibernetičku sigurnost opskrbnog lanca (2022.) – preporuke za prepoznavanje kritičnih dobavljača i upravljanje povezanim rizicima

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022