					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P41					Naslov dokumenta: **Politika upravljanja tveganj odvisnosti od dobaviteljev**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
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	
Uredba (EU) GDPR	čl. 28, čl. 32(1)(d)	
Direktiva (EU) NIS2	čl. 21(2)(d), čl. 21(3), čl. 22	
Uredba (EU) DORA	čl. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Namen

1.1 Okrepiti prakse varnosti dobavne verige v organizaciji z uvedbo postopka za prepoznavanje in upravljanje kritičnih odvisnosti od dobaviteljev in izvajalcev storitev, kot to zahtevata člen 21(3) Direktive (EU) NIS2 in usklajene ocene tveganj dobavne verige na ravni Unije.

1.2 Zagotoviti, da so tveganja, ki izhajajo iz koncentracije ali odvisnosti od posameznega dobavitelja, razumljena in ublažena ter da se v naše obvladovanje tveganj in načrtovanje neprekinjenega poslovanja vključijo vsa sektorsko specifična tveganja dobavne verige, kot jih opredelijo pristojni organi v skladu s členom 22 Direktive (EU) NIS2.

2. Področje uporabe

2.1 Ta politika velja za vse ključne dobavitelje in izvajalce storitev, od katerih je organizacija odvisna pri izvajanju kritičnih operacij, zlasti v dobavni verigi IKT (strojna oprema, programska oprema, storitve v oblaku, telekomunikacije, upravljane storitve).

2.2 Zajema notranje funkcije, vključno z nabavo, upravljanjem dobaviteljev, obvladovanjem tveganj in relevantnimi operativnimi oddelki. V obsegu zbiranja informacij o tveganjih vključuje tudi same dobavitelje. »Kritični dobavitelji« so tisti, katerih odpoved ali kompromitacija bi lahko pomembno vplivala na našo sposobnost izvajanja storitev ali izpolnjevanja pravnih obveznosti.

3. Cilji

3.1 Zagotoviti pregled nad odvisnostmi v dobavni verigi, zlasti z opredelitvijo posameznih točk odpovedi ali visokega tveganja koncentracije v naši bazi dobaviteljev (npr. odvisnost od enega ponudnika storitev v oblaku za vse storitve).

3.2 Uvesti ukrepe za zmanjšanje in upravljanje tveganj, povezanih z dobavitelji, kot so diverzifikacija, načrti ukrepanja ob nepredvidenih dogodkih ali zahteva po izboljšanih kontrolah pri dobaviteljih, ter s tem povečati odpornost proti odpovedim dobaviteljev ali napadom, ki izvirajo iz dobavne verige.

3.3 Uskladiti se z zahtevami Direktive (EU) NIS2 tako, da se rezultati vseh usklajenih presoj varnostnih tveganj kritičnih dobavnih verig (v skladu s členom 22) vključijo v organizacijske odločitve glede tveganj ter da je naš pristop k tveganjem dobavne verige dokumentiran in dokazljiv.

4. Vloge in odgovornosti

4.1 Funkcija upravljanja dobaviteljev (VMO): je skrbnik registra odvisnosti od dobaviteljev in usklajuje presoje tveganj. Zagotavlja, da se ob vključitvi in nato periodično vsak ključni dobavitelj presodi z vidika kritičnosti in ravni odvisnosti.

4.2 Funkcija obvladovanja tveganj (odbor za tveganja na ravni organizacije): pregleduje tveganje koncentracije in analize odvisnosti ter potrjuje strategije obravnave tveganj (npr. odobritev vključitve nadomestnega dobavitelja ali vzdrževanja dodatnih zalog kritičnih komponent). Tveganja dobavne verige vključuje v skupni register tveganj in o njih poroča najvišjemu vodstvu.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Spremljanje in revizija

9.1 Register odvisnosti in ocene tveganj so predmet letne notranje revizije. Notranja revizija preveri, ali so vsi kritični dobavitelji evidentirani, ali so njihove ocene tveganja posodobljene ter ali so načrti za zmanjševanje tveganj vzpostavljeni in se izvajajo. Preveri tudi, ali so bili ustrezno upoštevani zunanji vhodni podatki za presojo tveganj (poročila po členu 22 ipd.).

9.2 Učinkovitost ukrepov diverzifikacije in ukrepov ob nepredvidenih dogodkih se periodično testira. Na primer, izvede se lahko načrtovana simulacija, v kateri se predpostavi odpoved pomembnega dobavitelja, da se preizkusijo naši načrti neprekinjenega poslovanja in alternativne ureditve (podobno kot pri vaji DR, vendar za izpad dobavitelja). Rezultati teh testov se dokumentirajo, vse pomanjkljivosti pa se odpravijo.

9.3 Kazalniki: Funkcija obvladovanja tveganj spremlja kazalnike, kot sta »% kritičnih storitev, pri katerih je na voljo najmanj en nadomestni dobavitelj ali rešitev« ali »pet največjih odvisnosti od dobaviteljev in njihov trend tveganja«. Ti kazalniki se vključijo v nadzorne plošče tveganj za vodstvo. Cilj je trend zmanjševanja tveganja odvisnosti skozi čas; če kazalniki kažejo naraščanje odvisnosti, mora to sprožiti razpravo vodstva.

10. Pregled in vzdrževanje

10.1 To politiko najmanj enkrat letno pregledata ekipi za upravljanje dobaviteljev in obvladovanje tveganj. Pregled vključuje vse spremembe v okolju dobaviteljev (npr. če nov dobavitelj postane kritičen ali se obstoječega postopno opušča) ter vse nove regulativne zahteve glede zunanjega izvajanja ali tveganj tretjih oseb.

10.2 Če sektorski organi izdajo posodobljene smernice ali če incident razkrije vrzeli (na primer, če je imel izpad dobavitelja večji vpliv od pričakovanega, kar kaže, da je bila odvisnost v naši oceni tveganja napačno presojena), se politika posodobi zaradi natančnejših meril ali strategij zmanjševanja tveganj.

10.3 Revidirane različice politike mora odobriti najvišje vodstvo. O pomembnih spremembah se obvestijo vsi relevantni oddelki, gradiva za usposabljanje pa se ustrezno posodobijo, da odražajo nove postopke ali standarde.

11. Povezane politike in povezave

11.1 P01 – Politika informacijske varnosti. Določa odgovornost za upravljanje odvisnosti od dobaviteljev.

11.2 P02 – Politika upravljanja vlog in odgovornosti. Pojasnjuje lastništvo odločitev glede tveganj, povezanih z dobavitelji.

11.3 P06 – Politika upravljanja tveganj. Vključuje tveganje koncentracije v registre tveganj na ravni organizacije.

11.4 P26 – Politika varnosti tretjih oseb in dobaviteljev. Določa osnovne varnostne zahteve; P41 dodaja kontrole odvisnosti in koncentracije.

11.5 P27 – Politika uporabe storitev v oblaku. Uporablja merila odvisnosti pri vključevanju storitev v oblaku in načrtih izstopa.

11.6 P28 – Politika zunanjega razvoja. Obravnava tveganja odvisnosti pri zunanjem razvoju.

11.7 P32 – Politika neprekinjenega poslovanja in obnove po nesreči. Obravnava scenarije izpada dobavitelja oziroma njegove zamenjave.

11.8 P37 – Politika pravne in regulativne skladnosti. Zagotavlja, da pogodbe in obveznosti odražajo kontrole odvisnosti.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), člen 21(3) (zahteva upoštevanje ranljivosti, značilnih za vsakega neposrednega dobavitelja/izvajalca storitev, in kakovosti njihove kibernetske varnosti, vključno z rezultati usklajenih ocen tveganj dobavne verige)

12.2 Direktiva NIS2, člen 22(1) (usklajene ocene varnostnih tveganj kritičnih dobavnih verig na ravni Unije – subjekte obveščajo o tveganjih dobaviteljev na ravni sektorja)

12.3 Izvedbena uredba Komisije (EU) 2024/2690, Priloga, oddelek 5 (zahteve glede varnosti dobavne verige za subjekte, vključno z merili za izbor dobaviteljev, diverzifikacijo in pogodbenimi obveznostmi)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – priporočila za prepoznavanje kritičnih dobaviteljev in upravljanje povezanih tveganj

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