					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P41					Dokumenta nosaukums: **Piegādātāju atkarības riska pārvaldības politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
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	
ES VDAR	28. pants, 32. panta 1. punkta d) apakšpunkts	
ES NIS2	21. panta 2. punkta d) apakšpunkts, 21. panta 3. punkts, 22. pants	
ES DORA	28.–30. pants	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Mērķis

1.1 Pilnveidot organizācijas piegādes ķēdes drošības praksi, ieviešot procesu kritisko atkarību no piegādātājiem un pakalpojumu sniedzējiem identificēšanai un pārvaldībai, kā to nosaka NIS2 direktīvas 21. panta 3. punkts un Savienības līmeņa piegādes ķēdes risku izvērtējumi.

1.2 Nodrošināt, ka riski, kas izriet no koncentrācijas vai paļāvības uz vienu piegādātāju, tiek izprasti un mazināti, un ka visi nozarei specifiskie piegādes ķēdes riski, kurus iestādes identificējušas saskaņā ar NIS2 direktīvas 22. pantu, tiek iekļauti mūsu risku pārvaldībā un darbības nepārtrauktības plānošanā.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem būtiskajiem piegādātājiem un pakalpojumu sniedzējiem, uz kuriem organizācija paļaujas kritisku darbību nodrošināšanai, jo īpaši IKT piegādes ķēdē (aparatūra, programmatūra, mākoņpakalpojumi, telekomunikāciju pakalpojumi, pārvaldītie pakalpojumi).

2.2 Tā aptver iekšējās funkcijas, tostarp iepirkumu un piegādātāju pienācīgu pārbaudi, piegādātāju pārvaldību, risku pārvaldību un attiecīgās darbības struktūrvienības. Tā attiecas arī uz pašiem piegādātājiem tiktāl, ciktāl tas nepieciešams riska informācijas iegūšanai. “Kritiskie piegādātāji” ir tie, kuru atteice vai kompromitēšana var būtiski ietekmēt mūsu spēju sniegt pakalpojumus vai izpildīt tiesiskos pienākumus.

3. Mērķi

3.1 Nodrošināt pārskatāmību par piegādes ķēdes atkarībām, jo īpaši identificējot vienotos atteices punktus vai augstu koncentrācijas risku mūsu piegādātāju portfelī (piemēram, atkarību no viena mākoņpakalpojumu sniedzēja visu pakalpojumu nodrošināšanai).

3.2 Ieviest pasākumus piegādātāju risku mazināšanai un pārvaldībai, piemēram, diversifikāciju, ārkārtas rīcības plānus vai prasību pastiprināšanu attiecībā uz piegādātāju kontroles pasākumiem, tādējādi stiprinot noturību pret piegādātāju atteicēm vai piegādes ķēdes izraisītiem uzbrukumiem.

3.3 Nodrošināt atbilstību NIS2 prasībām, integrējot jebkuru koordinētu kritisko piegādes ķēžu drošības risku izvērtējumu rezultātus (saskaņā ar 22. pantu) organizācijas risku lēmumos un nodrošinot, ka mūsu pieeja piegādes ķēdes riskam ir dokumentēta un pierādāma.

4. Lomas un pienākumi

4.1 Piegādātāju pārvaldības birojs (VMO): atbild par piegādātāju atkarību reģistra uzturēšanu un koordinē risku izvērtēšanu. Nodrošina, ka katrs būtiskais piegādātājs tiek izvērtēts pēc kritiskuma un atkarības līmeņa pieņemšanas procesā un periodiski pēc tam.

4.2 Risku pārvaldība (uzņēmuma risku komiteja): pārskata koncentrācijas risku un atkarību analīzi, apstiprina riska apstrādes stratēģijas (piemēram, alternatīva piegādātāja piesaisti vai papildu krājumu uzturēšanu kritiskām komponentēm). Iekļauj piegādes ķēdes riskus kopējā risku reģistrā un ziņo izpildvadībai.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Uzraudzība un audits

9.1 Atkarību reģistrs un risku izvērtējumi tiek pakļauti iekšējam auditam vismaz reizi gadā. Iekšējais audits pārbauda, vai visi kritiskie piegādātāji ir uzskaitīti, vai to riska novērtējumi ir aktuāli un vai riska mazināšanas plāni ir ieviesti un tiek virzīti uz priekšu. Tiek pārbaudīts arī, vai ir pienācīgi ņemti vērā ārējo risku izvērtējumu ievaddati (22. panta ziņojumi u. c.).

9.2 Diversifikācijas un ārkārtas pasākumu efektivitāte tiek periodiski testēta. Piemēram, var tikt veikta plānota simulācija, kurā tiek pieņemts, ka būtisks piegādātājs nespēj nodrošināt pakalpojumu, lai testētu mūsu nepārtrauktības plānus un alternatīvos risinājumus (līdzīgi kā avārijas atjaunošanas mācībās, bet piegādātāja pakalpojumu nepieejamības scenārijam). Šo testu rezultāti tiek dokumentēti, un visas nepilnības tiek novērstas.

9.3 Metrikas: risku pārvaldības funkcija uzrauga tādas metrikas kā “% kritisko pakalpojumu, kuriem pieejams vismaz viens alternatīvs piegādātājs vai risinājums” vai “5 būtiskākās piegādātāju atkarības un to riska tendence”. Šīs metrikas tiek iekļautas risku informācijas panelī vadībai. Mērķis ir atkarības riska samazināšanās laika gaitā; ja metrikas rāda pieaugošu atkarību, tam jārosina vadības diskusija.

10. Pārskatīšana un uzturēšana

10.1 Šī politika vismaz reizi gadā jāpārskata piegādātāju pārvaldības un risku pārvaldības komandām. Pārskatīšanā jāņem vērā jebkādas izmaiņas piegādātāju vidē (piemēram, ja jauns piegādātājs kļūst kritisks vai esošais tiek pakāpeniski aizstāts) un jebkādas jaunas regulatīvās prasības attiecībā uz ārpakalpojumiem vai trešo pušu risku.

10.2 Ja nozares iestādes izdod atjauninātas vadlīnijas vai incidents atklāj trūkumus (piemēram, ja piegādātāja pakalpojumu nepieejamībai bija lielāka ietekme nekā prognozēts, norādot, ka mūsu risku izvērtēšanā atkarība novērtēta neprecīzi), politika jāatjaunina, precizējot kritērijus vai riska mazināšanas stratēģijas.

10.3 Pārskatītās politikas versijas jāapstiprina izpildvadībai. Par būtiskām izmaiņām jāpaziņo visām attiecīgajām struktūrvienībām, un apmācību materiāli attiecīgi jāatjaunina, lai atspoguļotu jaunās procedūras vai standartus.

11. Saistītās politikas un sasaiste

11.1 P01 – Informācijas drošības politika. Nosaka pārskatatbildību par piegādātāju atkarības pārvaldību.

11.2 P02 – Pārvaldības lomu un atbildību politika. Precizē atbildību par lēmumiem attiecībā uz piegādātāju risku.

11.3 P06 – Risku pārvaldības politika. Iekļauj koncentrācijas risku uzņēmuma risku reģistros.

11.4 P26 – Trešo pušu un piegādātāju drošības politika. Nosaka drošības pamatlīmeni; P41 papildina to ar atkarības un koncentrācijas kontroles pasākumiem.

11.5 P27 – Mākoņpakalpojumu izmantošanas politika. Piemēro atkarības kritērijus mākoņpakalpojumu ieviešanai un izstāšanās plāniem.

11.6 P28 – Ārpakalpojuma izstrādes politika. Aptver atkarības riskus ārējā inženierijā.

11.7 P32 – Darbības nepārtrauktības un avārijas atjaunošanas politika. Ietver plānošanu piegādātāja pakalpojumu nepieejamības un aizstāšanas scenārijiem.

11.8 P37 – Juridisko lietu un regulatīvās atbilstības politika. Nodrošina, ka līgumi un pienākumi atspoguļo atkarības kontroles pasākumus.

12. Atsauces

12.1 NIS2 direktīva (ES 2022/2555), 21. panta 3. punkts (nosaka pienākumu ņemt vērā katram tiešajam piegādātājam/pakalpojumu sniedzējam raksturīgās ievainojamības un to kiberdrošības kvalitāti, tostarp koordinētu piegādes ķēdes risku izvērtējumu rezultātus)

12.2 NIS2 direktīva, 22. panta 1. punkts (Savienības līmeņa koordinēti kritisko piegādes ķēžu drošības risku izvērtējumi — informē organizācijas par nozares mēroga piegādātāju riskiem)

12.3 Komisijas Īstenošanas regula (ES) 2024/2690, pielikuma 5. iedaļa (piegādes ķēdes drošības prasības organizācijām, tostarp kritēriji piegādātāju atlasei, diversifikācijai un līgumiskajām saistībām)

12.4 ENISA labā prakse piegādes ķēdes kiberdrošībā (2022) – ieteikumi kritisko piegādātāju identificēšanai un saistīto risku pārvaldībai

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