					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P41					Dokumento pavadinimas: **Tiekėjų priklausomybės rizikos valdymo politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

1. Tikslas

1.1 Sustiprinti organizacijos tiekimo grandinės saugumo praktiką, įdiegiant procesą, skirtą kritinėms priklausomybėms nuo tiekėjų ir paslaugų teikėjų nustatyti ir valdyti, kaip to reikalauja NIS2 direktyvos 21 straipsnio 3 dalis ir Sąjungos lygmens tiekimo grandinės rizikos vertinimai.

1.2 Užtikrinti, kad rizikos, kylančios dėl koncentracijos arba priklausomybės nuo vieno tiekėjo, būtų suprantamos ir mažinamos, o bet kokios konkrečiam sektoriui būdingos tiekimo grandinės rizikos, kaip nurodo institucijos pagal NIS2 direktyvos 22 straipsnį, būtų įtrauktos į mūsų rizikos valdymą ir veiklos tęstinumo planavimą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems kritiniams tiekėjams ir paslaugų teikėjams, nuo kurių organizacija priklauso vykdydama kritines operacijas, ypač IRT tiekimo grandinėje (aparatinė įranga, programinė įranga, debesijos paslaugos, telekomunikacijos, valdomosios paslaugos).

2.2 Ji apima vidaus funkcijas, įskaitant pirkimus, tiekėjų valdymą, rizikos valdymą ir atitinkamus veiklos padalinius. Ji taip pat taikoma patiems tiekėjams tiek, kiek tai susiję su rizikos informacijos teikimu. „Kritiniai tiekėjai“ yra tie, kurių veiklos sutrikimas ar kompromitavimas galėtų reikšmingai paveikti mūsų gebėjimą teikti paslaugas arba vykdyti teisinius įsipareigojimus.

3. Tikslai

3.1 Užtikrinti tiekimo grandinės priklausomybių matomumą, visų pirma nustatant vienintelį gedimo tašką arba didelę koncentracijos riziką tiekėjų portfelyje (pvz., priklausomybę nuo vieno debesijos paslaugų teikėjo visoms paslaugoms).

3.2 Įgyvendinti priemones tiekėjų rizikai mažinti ir valdyti, pavyzdžiui, diversifikavimą, nenumatytų atvejų planus arba reikalavimą stiprinti tiekėjo kontrolės priemones, taip didinant atsparumą tiekėjo veiklos sutrikimams ar iš tiekimo grandinės kylančioms atakoms.

3.3 Užtikrinti atitiktį NIS2 direktyvos reikalavimams, integruojant bet kokių koordinuotų kritinių tiekimo grandinių saugumo rizikos vertinimų rezultatus (pagal 22 straipsnį) į organizacijos sprendimus dėl rizikos ir užtikrinant, kad mūsų tiekimo grandinės rizikos valdymo metodas būtų dokumentuotas ir pagrįstas.

4. Vaidmenys ir atsakomybės

4.1 Tiekėjų valdymo funkcija (VMO): valdo tiekėjų priklausomybės registrą ir koordinuoja rizikos vertinimus. Užtikrina, kad priėmimo etape ir vėliau periodiškai kiekvienas pagrindinis tiekėjas būtų įvertintas pagal kritiškumą ir priklausomybės lygį.

4.2 Rizikos valdymo funkcija (įmonės rizikos komitetas): peržiūri koncentracijos riziką ir priklausomybės analizes, tvirtina rizikos valdymo strategijas (pvz., pritaria alternatyvaus tiekėjo įtraukimui arba papildomų atsargų palaikymui kritiniams komponentams). Įtraukia tiekimo grandinės riziką į bendrą rizikų registrą ir teikia informaciją aukščiausiajai vadovybei.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Stebėsena ir auditas

9.1 Priklausomybės registras ir rizikos vertinimai kasmet turi būti audituojami vidaus tvarka. Vidaus audito komanda tikrins, ar visi kritiniai tiekėjai yra įtraukti, ar jų rizikos vertinimai yra aktualūs ir ar yra parengti bei vykdomi rizikos mažinimo planai. Taip pat bus tikrinama, ar išorinių rizikos vertinimų įvestys (22 straipsnio ataskaitos ir pan.) buvo tinkamai įvertintos.

9.2 Diversifikavimo ir nenumatytų atvejų priemonių veiksmingumas turi būti periodiškai testuojamas. Pavyzdžiui, gali būti atliekama planinė simuliacija, darant prielaidą, kad reikšmingo tiekėjo veikla sutriko, siekiant patikrinti mūsų veiklos tęstinumo planus ir alternatyvius susitarimus (panašiai kaip DR pratybos, tačiau tiekėjo sutrikimo scenarijui). Šių testų rezultatai dokumentuojami, o visi trūkumai pašalinami.

9.3 Rodikliai: Rizikos valdymo funkcija stebi tokius rodiklius kaip „% kritinių paslaugų, kurioms yra bent vienas alternatyvus tiekėjas arba sprendimas“ arba „5 didžiausios tiekėjų priklausomybės ir jų rizikos tendencija“. Šie rodikliai turi būti įtraukti į vadovybei teikiamą rizikos suvestinę. Priklausomybės rizikos mažėjimo tendencija laikui bėgant yra siektina; jei rodikliai rodo didėjančią priklausomybę, tai turi inicijuoti vadovybės svarstymą.

10. Peržiūra ir priežiūra

10.1 Šią politiką ne rečiau kaip kartą per metus peržiūri tiekėjų valdymo ir rizikos valdymo komandos. Peržiūros metu turi būti įvertinti visi tiekėjų aplinkos pokyčiai (pvz., jei naujas tiekėjas tampa kritinis arba senojo palaipsniui atsisakoma) ir visi nauji išorės paslaugų ar trečiųjų šalių rizikos reglamentavimo reikalavimai.

10.2 Jei sektoriaus institucijos paskelbia atnaujintas gaires arba incidentas atskleidžia spragas (pavyzdžiui, jei tiekėjo sutrikimas turėjo didesnį poveikį, nei buvo numatyta, ir tai rodo, kad mūsų rizikos vertinimas neteisingai įvertino priklausomybę), politika turi būti atnaujinta, patikslinant kriterijus arba rizikos mažinimo strategijas.

10.3 Atnaujintas politikos versijas turi patvirtinti aukščiausioji vadovybė. Apie reikšmingus pakeitimus turi būti informuoti visi susiję padaliniai, o mokymo medžiaga turi būti atitinkamai atnaujinta, kad atspindėtų naujas procedūras ar standartus.

11. Susijusios politikos ir sąsajos

11.1 P01 – Informacijos saugumo politika. Nustato atskaitomybę už tiekėjų priklausomybės valdyseną.

11.2 P02 – Valdysenos vaidmenų ir atsakomybių politika. Patikslina atsakomybių priskyrimą priimant sprendimus dėl tiekėjų rizikos.

11.3 P06 – Rizikos valdymo politika. Įtraukia koncentracijos riziką į įmonės rizikų registrus.

11.4 P26 – Trečiųjų šalių ir tiekėjų saugumo politika. Nustato bazines saugumo priemones; P41 jas papildo priklausomybės ir koncentracijos kontrolės priemonėmis.

11.5 P27 – Debesijos paslaugų naudojimo politika. Taiko priklausomybės kriterijus debesijos paslaugų pasirinkimui ir pasitraukimo planams.

11.6 P28 – Išorės vystymo politika. Apima priklausomybės riziką išorės inžinerinėje veikloje.

11.7 P32 – Veiklos tęstinumo ir atkūrimo po katastrofos politika. Nustato planavimą tiekėjo sutrikimo / pakeitimo scenarijams.

11.8 P37 – Teisinės ir reguliacinės atitikties politika. Užtikrina, kad sutartys ir įsipareigojimai atspindėtų priklausomybės kontrolės priemones.

12. Nuorodos

12.1 NIS2 direktyva (ES 2022/2555), 21 straipsnio 3 dalis (reikalaujanti atsižvelgti į kiekvienam tiesioginiam tiekėjui / paslaugų teikėjui būdingus pažeidžiamumus ir jų kibernetinio saugumo kokybę, įskaitant koordinuotų tiekimo grandinės rizikos vertinimų rezultatus)

12.2 NIS2 direktyva, 22 straipsnio 1 dalis (Sąjungos lygmens koordinuoti kritinių tiekimo grandinių saugumo rizikos vertinimai – informuoja subjektus apie viso sektoriaus tiekėjų riziką)

12.3 Komisijos įgyvendinimo reglamentas (ES) 2024/2690, priedo 5 skirsnis (tiekimo grandinės saugumo reikalavimai subjektams, įskaitant tiekėjų pasirinkimo, diversifikavimo ir sutartinių įsipareigojimų kriterijus)

12.4 ENISA gerosios tiekimo grandinės kibernetinio saugumo praktikos (2022) – rekomendacijos dėl kritinių tiekėjų nustatymo ir susijusių rizikų valdymo

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