					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P41					Dokumenttitel: **Politik for risikostyring af leverandørafhængigheder**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
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	
EU GDPR	Art. 28, Art. 32(1)(d)	
EU NIS2	Art. 21(2)(d), Art. 21(3), Art. 22	
EU DORA	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Formål

1.1 At styrke organisationens sikkerhed i forsyningskæden ved at etablere en proces til at identificere og styre kritiske afhængigheder af leverandører og tjenesteudbydere, som krævet efter NIS2 artikel 21, stk. 3, og risikovurderinger af forsyningskæden på EU-plan.

1.2 At sikre, at risici som følge af koncentrationsrisiko eller afhængighed af eneleverandører forstås og begrænses, og at eventuelle sektorspecifikke risici i forsyningskæden, som fremhævet af myndigheder efter NIS2 artikel 22, indarbejdes i vores risikostyring og planlægning af forretningskontinuitet.

2. Omfang

2.1 Denne politik gælder for alle væsentlige leverandører og tjenesteudbydere, som organisationen er afhængig af for kritiske driftsaktiviteter, særligt i IKT-forsyningskæden (hardware, software, cloudtjenester, telekommunikation, managed services).

2.2 Den omfatter interne funktioner, herunder indkøb og leverandørdue diligence, Vendor Management Office (VMO), risikostyring og relevante driftsafdelinger. Den omfatter også leverandørerne selv i det omfang, det er nødvendigt for at indhente risikooplysninger. "Kritiske leverandører" er leverandører, hvis svigt eller kompromittering væsentligt kan påvirke vores evne til at levere tjenester eller opfylde retlige forpligtelser.

3. Mål

3.1 At opnå overblik over afhængigheder i forsyningskæden, herunder især at identificere afhængigheder med enkeltfejlspunkter eller høj koncentrationsrisiko i leverandørgrundlaget (f.eks. afhængighed af én cloududbyder til alle tjenester).

3.2 At implementere foranstaltninger til at reducere og styre leverandørrelaterede risici, såsom diversificering, beredskabsplaner eller krav om forbedrede leverandørkontroller, og dermed styrke robustheden over for leverandørsvigt eller angreb med oprindelse i forsyningskæden.

3.3 At sikre tilpasning til NIS2-krav ved at integrere resultater fra koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, jf. artikel 22, i organisationens risikobeslutninger og ved at sikre, at vores tilgang til risici i forsyningskæden er dokumenteret og kan dokumenteres.

4. Roller og ansvar

4.1 Vendor Management Office (VMO): Har ansvaret for registret over leverandørafhængigheder og koordinerer risikovurderinger. Sikrer, at hver nøgleleverandør ved onboarding og derefter periodisk vurderes med hensyn til kritikalitet og afhængighedsniveau.

4.2 Risikostyring (Enterprise Risk Committee): Gennemgår koncentrationsrisiko og analyser af leverandørafhængighed, godkender strategier for risikobehandling (f.eks. godkendelse af en alternativ leverandør eller ekstra lager af kritiske komponenter) og indarbejder risici i forsyningskæden i det overordnede risikoregister samt rapporterer til den øverste ledelse.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Overvågning og revision

9.1 Registret over leverandørafhængigheder og tilhørende risikovurderinger skal underkastes intern revision mindst én gang årligt. Intern revision skal verificere, at alle kritiske leverandører er registreret, at deres risikovurderinger er opdaterede, og at risikobehandlingsplaner er etableret og følges. Der skal også kontrolleres, at input fra eksterne risikovurderinger (rapporter efter artikel 22 mv.) er taget behørigt i betragtning.

9.2 Effektiviteten af diversificering og beredskabsforanstaltninger skal testes periodisk. Der kan f.eks. gennemføres en planlagt simulering, hvor en væsentlig leverandør antages at svigte, for at teste vores planer for forretningskontinuitet og alternative ordninger (på samme måde som en DR-øvelse, men for leverandørsvigt). Resultaterne af disse test skal dokumenteres, og eventuelle mangler skal afhjælpes.

9.3 Metrikker: Risikostyringsfunktionen skal følge metrikker som f.eks. "% af kritiske tjenester med mindst én alternativ leverandør eller løsning tilgængelig" eller "Top 5 leverandørafhængigheder og deres risikotrend". Disse metrikker skal indgå i ledelsens risikodashboards. En faldende udvikling i afhængighedsrisiko over tid er et mål; hvis metrikkerne viser stigende afhængighed, skal det udløse ledelsesmæssig drøftelse.

10. Gennemgang og vedligeholdelse

10.1 Denne politik skal gennemgås mindst årligt af Vendor Management Office (VMO) og risikostyringsteams. Gennemgangen skal indarbejde ændringer i leverandørlandskabet (f.eks. hvis en ny leverandør bliver kritisk, eller en eksisterende udfases) samt nye regulatoriske krav til outsourcing eller tredjepartsrisiko.

10.2 Hvis sektormyndigheder udsteder opdateret vejledning, eller hvis en hændelse afdækker mangler (for eksempel hvis et leverandørsvigt havde større konsekvenser end forventet og dermed viser, at vores risikovurdering undervurderede afhængigheden), skal politikken opdateres for at præcisere kriterier eller strategier for risikoafbødning.

10.3 Reviderede versioner af politikken skal godkendes af den øverste ledelse. Væsentlige ændringer skal kommunikeres til alle relevante afdelinger, og træningsmateriale skal opdateres tilsvarende, så nye procedurer eller standarder afspejles.

11. Relaterede politikker og sammenhænge

11.1 P01 – Informationssikkerhedspolitik. Fastlægger ansvarlighed for styring af leverandørafhængigheder.

11.2 P02 – Politik for styringsroller og ansvarsområder. Tydeliggør ejerskab for beslutninger om leverandørrisiko.

11.3 P06 – Politik for risikostyring. Indarbejder koncentrationsrisiko i organisationens risikoregistre.

11.4 P26 – Politik for tredjeparts- og leverandørsikkerhed. Fastlægger grundlæggende sikkerhedskrav; P41 tilføjer kontroller for afhængighed og koncentration.

11.5 P27 – Politik for brug af cloudtjenester. Anvender afhængighedskriterier ved anvendelse af cloudtjenester og planlægning af leverandørskifte.

11.6 P28 – Politik for outsourced udvikling. Omfatter afhængighedsrisici i ekstern udvikling.

11.7 P32 – Politik for forretningskontinuitet og genopretning efter alvorlige hændelser. Planlægger for scenarier med leverandørsvigt eller leverandørsubstitution.

11.8 P37 – Politik for juridisk og regulatorisk efterlevelse. Sikrer, at kontrakter og forpligtelser afspejler kontroller for leverandørafhængighed.

12. Referencer

12.1 NIS2-direktivet (EU 2022/2555), artikel 21, stk. 3 (krav om at tage hensyn til sårbarheder, der er specifikke for hver direkte leverandør/tjenesteudbyder, og kvaliteten af deres cybersikkerhed, herunder resultater af koordinerede risikovurderinger af forsyningskæden)

12.2 NIS2-direktivet, artikel 22, stk. 1 (koordinerede sikkerhedsrisikovurderinger på EU-plan af kritiske forsyningskæder – informerer enheder om sektoromfattende leverandørrisici)

12.3 Kommissionens gennemførelsesforordning (EU) 2024/2690, bilag afsnit 5 (krav til sikkerhed i forsyningskæden for enheder, herunder kriterier for leverandørvalg, diversificering og kontraktlige forpligtelser)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – anbefalinger om identifikation af kritiske leverandører og styring af relaterede risici

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