					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P41					Dokumenttitel: **Policy för hantering av risker kopplade till leverantörsberoenden**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassad till standarder och regelverk

Standard/reglering	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:s GDPR	Art. 28, Art. 32(1)(d)	
EU:s NIS2-direktiv	Art. 21(2)(d), Art. 21(3), Art. 22	
EU:s DORA-förordning	Art. 28–30	
COBIT 2019	APO10.01, APO10.02, APO10.03, APO10.04, DSS04.07, MEA02.03	

1. Syfte

1.1 Stärka organisationens praxis för säkerhet i leveranskedjan genom att införa en process för att identifiera och hantera kritiska beroenden av leverantörer och tjänsteleverantörer, i enlighet med artikel 21.3 i EU:s NIS2-direktiv och unionsövergripande riskbedömningar av leveranskedjan.

1.2 Säkerställa att risker som uppstår till följd av koncentration till eller beroende av enskilda leverantörer förstås och reduceras, samt att eventuella sektorsspecifika risker i leveranskedjan, såsom uppmärksammats av myndigheter enligt artikel 22 i NIS2, införlivas i vår riskhantering och planering för verksametskontinuitet.

2. Omfattning

2.1 Denna policy gäller för alla väsentliga leverantörer och tjänsteleverantörer som organisationen är beroende av för verksamhetskritiska funktioner, särskilt inom IKT-leveranskedjan (hårdvara, programvara, molntjänster, telekommunikation och hanterade tjänster).

2.2 Den omfattar interna funktioner, inklusive Upphandling, leverantörsstyrning, Riskhantering och relevanta operativa enheter. Den omfattar även leverantörerna själva i den utsträckning det krävs för att samla in riskinformation. Med "kritiska leverantörer" avses leverantörer vars bortfall eller kompromettering väsentligt skulle kunna påverka vår förmåga att leverera tjänster eller uppfylla rättsliga skyldigheter.

3. Mål

3.1 Skapa överblick över beroenden i leveranskedjan, särskilt genom att identifiera enskilda felpunkter eller hög koncentrationsrisk i leverantörsbasen (t.ex. beroende av en molnleverantör för samtliga tjänster).

3.2 Införa åtgärder för att reducera och hantera leverantörsrelaterade risker, såsom diversifiering, reservlösningar eller krav på förstärkta kontroller hos leverantören, och därigenom stärka motståndskraften mot leverantörsbortfall eller angrepp med ursprung i leveranskedjan.

3.3 Anpassa verksamheten till kraven i EU:s NIS2-direktiv genom att integrera resultaten från samordnade säkerhetsriskbedömningar av kritiska leveranskedjor enligt artikel 22 i organisationens riskbeslut samt säkerställa att vår metod för hantering av leveranskedjerisker är dokumenterad och kan uppvisas.

4. Roller och ansvar

4.1 Vendor Management Office (VMO): Ansvarar för registret över leverantörsberoenden och samordnar riskbedömningar. Säkerställer att varje nyckelleverantör bedöms avseende kritikalitet och beroendenivå vid leverantörsintroduktion och därefter periodiskt.

4.2 Riskhantering (Enterprise Risk Committee): Granskar koncentrationsrisker och beroendeanalyser, godkänner strategier för riskbehandling (t.ex. att lägga till en alternativ leverantör eller hålla extra lager av kritiska komponenter). Införlivar risker i leveranskedjan i det övergripande riskregistret och rapporterar till högsta ledningen.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Övervakning och revision

9.1 Registret över leverantörsberoenden och riskbedömningarna ska internrevideras årligen. Internrevision ska verifiera att alla kritiska leverantörer är förtecknade, att deras riskklassningar är aktuella och att riskreducerande planer finns på plats och fortskrider. Internrevision ska även kontrollera att externa underlag från riskbedömningar (rapporter enligt artikel 22 etc.) har beaktats på ett ändamålsenligt sätt.

9.2 Effektiviteten i åtgärder för diversifiering och kontinuitet ska testas periodiskt. Exempelvis kan en planerad simulering genomföras där en större leverantör antas fallera för att pröva våra planer för verksametskontinuitet och alternativa lösningar (liknande en katastrofåterställningsövning men för leverantörsbortfall). Resultaten av dessa tester ska dokumenteras och eventuella brister åtgärdas.

9.3 Mätetal: Riskhantering ska följa upp mätetal såsom "% av kritiska tjänster där minst en alternativ leverantör eller lösning finns tillgänglig" eller "De fem största leverantörsberoendena och deras risktrend". Dessa mätetal ska inkluderas i riskrapporteringen till ledningen. En nedåtgående trend i beroenderisk över tid är ett mål. Om mätetalen visar ökande beroende ska detta utlösa diskussion i ledningen.

10. Granskning och underhåll

10.1 Denna policy ska granskas minst årligen av teamen för leverantörsstyrning och Riskhantering. Granskningen ska beakta förändringar i leverantörslandskapet (t.ex. om en ny leverantör blir kritisk eller en tidigare leverantör avvecklas) samt nya regulatoriska krav avseende outsourcing eller tredjepartsrisker.

10.2 Om sektorsmyndigheter utfärdar uppdaterad vägledning eller om en incident visar på brister (till exempel om ett leverantörsavbrott fick större påverkan än förväntat, vilket indikerar att vår riskbedömning felbedömde beroendet), ska policyn uppdateras för att förfina kriterier eller strategier för riskreducering.

10.3 Reviderade versioner av policyn ska godkännas av högsta ledningen. Betydande förändringar ska kommuniceras till alla relevanta avdelningar, och utbildningsmaterial ska uppdateras i enlighet med detta för att återspegla nya rutiner eller standarder.

11. Relaterade policyer och kopplingar

11.1 P01 – Informationssäkerhetspolicy. Tilldelar ansvarsskyldighet för styrning av leverantörsberoenden.

11.2 P02 – Policy för styrningsroller och ansvar. Förtydligar ägarskap för beslut om leverantörsrisker.

11.3 P06 – Riskhanteringspolicy. Införlivar koncentrationsrisk i organisationens riskregister.

11.4 P26 – Policy för leverantörssäkerhet och tredjepartssäkerhet. Anger säkerhetsbaslinjen; P41 tillför kontroller för beroende och koncentration.

11.5 P27 – Policy för användning av molntjänster. Tillämpa kriterier för beroende vid införande av molntjänster och i exitplaner.

11.6 P28 – Policy för outsourcad utveckling. Omfattar beroenderisker inom extern utveckling.

11.7 P32 – Policy för verksamhetskontinuitet och katastrofåterställning. Planerar för scenarier med leverantörsbortfall eller leverantörsbyte.

11.8 P37 – Policy för rättslig och regulatorisk efterlevnad. Säkerställer att avtal och skyldigheter återspeglar kontroller för leverantörsberoenden.

12. Referenser

12.1 NIS2-direktivet (EU 2022/2555), artikel 21.3 (kräver att sårbarheter som är specifika för varje direkt leverantör/tjänsteleverantör och kvaliteten i deras cybersäkerhet beaktas, inklusive resultat från samordnade riskbedömningar av leveranskedjan)

12.2 NIS2-direktivet, artikel 22.1 (unionsövergripande samordnade säkerhetsriskbedömningar av kritiska leveranskedjor – informerar organisationer om sektorsövergripande leverantörsrisker)

12.3 Kommissionens genomförandeförordning (EU) 2024/2690, bilaga avsnitt 5 (krav på säkerhet i leveranskedjan för organisationer, inklusive kriterier för val av leverantör, diversifiering och avtalskrav)

12.4 ENISA Good Practices for Supply Chain Cybersecurity (2022) – rekommendationer för att identifiera kritiska leverantörer och hantera tillhörande risker

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