					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P26					Dokumenttitel: **Politik for tredjeparts- og leverandørsikkerhed**							
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	Clause 8	Operationel planlægning og styring: Kræver formelle kontroller for tredjepartstjenester, der påvirker ISMS'et
ISO/IEC 27002:2022	Controls 5.19–5.22	Politikker og procedurer for leverandørforhold; styring af leverandørrisici; styring af levering af leverandørtjenester; overvågning og gennemgang af leverandører
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Eksterne systemtjenester; konfigurationsstyring for udviklere; systemforbindelser; personalesikkerhed for tredjeparter
EU GDPR	Articles 28, 32, 33	Forpligtelser for databehandlere, behandlingssikkerhed, underretning om brud på persondatasikkerheden
EU NIS2	Article 21(2)(e–f)	Risikobaseret leverandørstyring og sikkerhedstilsyn
EU DORA	Articles 28, 30	IKT-tredjepartsrisiko, tilsyn med kritiske IKT-tredjepartsudbydere
COBIT 2019	BAI05, DSS02, MEA03	Styring af organisatorisk ændringsimplementering; styring af serviceanmodninger og hændelser; overvågning, evaluering og vurdering af efterlevelse

1. Formål

1.1 Denne politik fastlægger krav til informationssikkerhed ved etablering, styring og opretholdelse af sikre relationer med tredjepartsleverandører og tjenesteudbydere.

1.2 Den sikrer, at alle leverandører med adgang til organisationens data, systemer eller infrastruktur er underlagt stringente sikkerhedskontroller, kontraktuelle sikkerhedsforanstaltninger og løbende tilsyn gennem hele tjenestens livscyklus.

1.3 Politikken understøtter kontrollerne i ISO/IEC 27001 Annex A, 5.19 til 5.22, ved at indarbejde sikkerhedskrav i indkøb, onboarding, due diligence, kontraktstyring, serviceovervågning og offboarding.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle tredjepartsleverandører, kontraktparter, cloududbydere og serviceorganisationer, der behandler eller har adgang til organisationens informationsaktiver

2.1.2 Alle interne roller, der indgår i leverandørevaluering, onboarding, kontraktindgåelse, risikostyring, overvågning eller ophør

2.1.3 Alle leverandørforhold, som omfatter adgang til følsomme data, integration med produktionsmiljøer eller understøttelse af kritiske forretningsfunktioner

2.2 Politikken omfatter både direkte leverandører og deres underleverandører, hvor det er relevant, og inkluderer tredjepartssoftware, infrastruktur, support og administrerede tjenester.

3. Mål

3.1 Sikre, at leverandørsikkerhedsrisici identificeres, vurderes og afbødes ensartet gennem hele relationens livscyklus.

3.2 Indarbejde standardiserede sikkerhedskrav i alle leverandørkontrakter, herunder forpligtelser vedrørende underretning om brud, klausuler om revisionsret og ansvar for databeskyttelse.

3.3 Kræve formel due diligence og dokumenterede risikovurderinger, før nye leverandører engageres, eller højrisikoaftaler fornys.

3.4 Etablere mekanismer til løbende overvågning af leverandørers efterlevelse, herunder performancegennemgange, revisioner og eskalering af hændelser.

3.5 Styre ændringer i leverandørtjenester og sikre kontrolleret offboarding samt returnering eller destruktion af data ved ophør.

3.6 Tilpasse tredjepartssikkerhedskontroller til gældende regulatoriske og kontraktuelle forpligtelser, herunder GDPR, NIS2, DORA og ISO/IEC 27001.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer, at den er afstemt med det samlede ISMS, risikostyring og efterlevelsesstrategi.

4.1.2 Godkender niveauer for leverandørklassificering, resultater af sikkerhedsgennemgange og undtagelser for højrisikoleverandører.

4.1.3 Deltager i eskalering af alvorlige leverandørhændelser og kontraktforhandlinger vedrørende kritiske tjenester.

4.2 Indkøb og leverandørstyring

4.2.1 Sikrer, at alle nye og fornyede leverandørkontrakter indeholder godkendte sikkerheds- og databeskyttelsesklausuler.

4.2.2 Vedligeholder det centrale leverandørregister og koordinerer med Juridisk afdeling og Compliance om dokumentation for tredjepartsrisici.

4.2.3 Iværksætter onboardingprocesser og sikrer afstemning med sikkerhedsvurderinger før kontraktindgåelse.

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

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt eller tidligere i tilfælde af:

9.1.1 Væsentlige ændringer i indkøbsstrategi eller leverandørøkosystem

9.1.2 Opdateringer af juridiske eller regulatoriske rammer (f.eks. DORA, GDPR)

9.1.3 Større tredjepartshændelser, brud på persondatasikkerheden eller revisionssvigt

9.1.4 Konstateringer fra risikovurderinger eller eksterne certificeringsorganer

9.2 Gennemgangsprocessen ejes i fællesskab af CISO, Indkøb, Juridisk afdeling og risikostyringsfunktionerne.

9.3 Alle revisioner af politikken skal dokumenteres i ISMS'ets dokumentstyringsregister, være versionsstyrede og kommunikeres til relevante interessenter gennem kanaler for leverandørstyring og programmer for sikkerhedsbevidsthed for medarbejdere.

9.4 Erstattede versioner skal arkiveres i mindst tre år af hensyn til sporbarhed og juridisk efterlevelse.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger den overordnede forpligtelse til at sikre alle organisatoriske aktiviteter, herunder afhængigheder af tredjepartsleverandører og eksterne tjenesteudbydere.

10.2 P6 – Politik for risikostyring. Vejleder i identifikation, vurdering og afbødning af risici forbundet med tredjepartsforhold, herunder nedarvede eller systemiske risici fra leverandørøkosystemer.

10.3 P17 – Databeskyttelses- og privatlivspolitik. Gælder for alle leverandører, der håndterer personoplysninger, og kræver passende kontraktvilkår, sikkerhedsforanstaltninger ved overførsler og principper om databeskyttelse gennem design.

10.4 P4 – Politik for adgangskontrol. Regulerer, hvordan tredjepartspersonale får adgang til organisationens systemer, og håndhæver rollebaserede tilladelser, sessionskontroller og procedurer for tilbagekaldelse.

10.5 P22 – Lognings- og overvågningspolitik. Kræver, at leverandørers adgang til systemer overvåges, logges og gennemgås, særligt i miljøer, hvor privilegerede eller datacentrerede aktiviteter forekommer.

10.6 P30 – Politik for hændelseshåndtering. Fastlægger eskalationsprocedurer og krav til rapportering af brud for sikkerhedshændelser med oprindelse hos leverandører eller fælles undersøgelser, der involverer tredjepartssystemer.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001: Clause 8.1 – Operationel planlægning og styring: Kræver formelle kontroller for tredjepartstjenester, der påvirker ISMS'et.

11.2 ISO/IEC 27002:2022 – Controls 5.19 to 5.22:

11.2.1 Annex A Control 5.19 – Politikker og procedurer for leverandørforhold: Pålægger kontroller til styring af interaktioner med leverandører.

11.2.2 Annex A Control 5.20 – Styring af leverandørrisici: Fokuserer på identifikation, vurdering og løbende tilsyn med leverandørers sikkerhedstilstand.

11.2.3 Annex A Control 5.21 – Styring af levering af leverandørtjenester: Kræver, at performance og sikkerhed er afstemt med kontraktuelle forventninger.

11.2.4 Annex A Control 5.22 – Overvågning og gennemgang af leverandører: Understreger behovet for løbende validering og revurdering af tredjeparters efterlevelse.

11.3 NIST SP 800-53 Rev.:

11.3.1 SA-9 – Eksterne systemtjenester: Definerer krav til sikkerhed og risiko for systemer, der drives af eksterne enheder.

11.3.2 SA-10 – Konfigurationsstyring for udviklere: Gælder, når tredjeparter leverer software eller miljøer.

11.3.3 CA-3 – Systemforbindelser: Kræver tilsyn med og aftaler om systemers dataflows mellem enheder.

11.3.4 PS-7 – Personalesikkerhed for tredjeparter: Sikrer, at kontraktparter og leverandørpersonale screenes og overvåges på passende vis.

11.4 EU GDPR (2016/679):

11.4.1 Article 28 – Forpligtelser for databehandlere: Kræver skriftlige aftaler med databehandlere, herunder tekniske og organisatoriske foranstaltninger.

11.4.2 Article 32 – Behandlingssikkerhed: Pålægger passende sikkerhedsforanstaltninger for både dataansvarlige og databehandlere.

11.4.3 Article 33 – Underretning om brud på persondatasikkerheden: Kræver hurtig underretning fra leverandører i tilfælde af brud.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Article 21(2)(e–f): Kræver risikobaseret leverandørstyring og sikkerhedstilsyn, særligt i væsentlige og vigtige enheders digitale forsyningskæder.

11.6 EU DORA (2022/2554):

11.6.1 Article 28 – IKT-tredjepartsrisiko: Pålægger krav om risikovurdering, kontraktuelle sikkerhedsvilkår og exitstrategier for udbydere af finansielle tjenester.

11.6.2 Article 30 – Tilsyn med kritiske IKT-tredjepartsudbydere: Etablerer skærpede forventninger til overvågning og tilsyn med nøgleleverandører.

11.7 COBIT 2019:

11.7.1 BAI05 – Styring af organisatorisk ændringsimplementering: Sikrer, at leverandørovergange styres sikkert.

11.7.2 DSS02 – Styring af serviceanmodninger og hændelser: Gælder for leverandørrapporterede problemer og integration med hændelseshåndtering.

11.7.3 MEA03 – Overvågning, evaluering og vurdering af efterlevelse: Understøtter måling af leverandørperformance og overvågning af efterlevelse.