					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P26					Dokumenttitel: **policy för leverantörssäkerhet och tredjepartssäkerhet**							
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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Operativ planering och styrning: Kräver formella kontroller för tredjepartstjänster som påverkar ISMS
ISO/IEC 27002:2022	Kontroller 5.19–5.22	Policyer och rutiner för leverantörsrelationer; hantering av leverantörsrisker; styrning av leverans av leverantörstjänster; övervakning och granskning av leverantörer
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Externa systemtjänster; utvecklares konfigurationshantering; systemsammanlänkningar; personalsäkerhet för tredje part
EU:s GDPR	Artiklarna 28, 32, 33	Skyldigheter för personuppgiftsbiträden; säkerhet i behandlingen; anmälan av personuppgiftsincidenter
EU:s NIS2-direktiv	Artikel 21.2 e–f	Riskbaserad leverantörshantering och säkerhetstillsyn
EU:s DORA-förordning	Artiklarna 28, 30	IKT-risker kopplade till tredje part; tillsyn av kritiska IKT-tredjepartsleverantörer
COBIT 2019	BAI05, DSS02, MEA03	Hantera organisatorisk förändringsförmåga; hantera servicebegäranden och incidenter; övervaka, utvärdera och bedöma regelefterlevnad

1. Syfte

1.1 Denna policy fastställer informationssäkerhetskrav för att etablera, hantera och upprätthålla säkra relationer med tredjepartsleverantörer och tjänsteleverantörer.

1.2 Den säkerställer att alla leverantörer med åtkomst till organisationens data, system eller infrastruktur omfattas av robusta säkerhetskontroller, avtalsmässiga skyddsåtgärder och kontinuerlig tillsyn under hela tjänstens livscykel.

1.3 Policyn stödjer kontrollerna 5.19 till 5.22 i bilaga A till ISO/IEC 27001 genom att integrera säkerhetskrav i upphandling, leverantörsintroduktion, leverantörsgranskning, avtalshantering, tjänsteövervakning och avvecklingsprocesser.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla tredjepartsleverantörer, entreprenörer, molntjänstleverantörer och tjänsteorganisationer som behandlar eller har åtkomst till organisationens informationstillgångar

2.1.2 Alla interna roller som deltar i leverantörsutvärdering, leverantörsintroduktion, avtalstecknande, riskhantering, övervakning eller avveckling

2.1.3 Alla leverantörsrelationer som omfattar åtkomst till känsliga data, integration med produktionsmiljöer eller stöd till kritiska verksamhetsfunktioner

2.2 Policyn omfattar både direkta leverantörer och deras underleverantörer där så är tillämpligt samt inkluderar programvara från tredje part, infrastruktur, support och managerade tjänster.

3. Mål

3.1 Säkerställa att leverantörsrisker konsekvent identifieras, bedöms och reduceras under hela relationens livscykel.

3.2 Integrera standardiserade säkerhetskrav i samtliga leverantörsavtal, inklusive skyldigheter att rapportera incidenter, villkor om revisionsrätt och ansvar för dataskydd.

3.3 Kräva formell leverantörsgranskning och dokumenterade riskbedömningar innan nya leverantörer anlitas eller tjänsteöverenskommelser med hög risk förnyas.

3.4 Etablera mekanismer för kontinuerlig efterlevnadsövervakning av leverantörer, inklusive prestationsbedömningar, revisioner och incidenteskalering.

3.5 Hantera ändringar i leverantörstjänster och säkerställa säker avveckling samt återlämning eller förstöring av data vid avslut.

3.6 Anpassa säkerhetskontroller för tredje part till tillämpliga regulatoriska skyldigheter och avtalskrav, inklusive EU:s GDPR, EU:s NIS2-direktiv, EU:s DORA-förordning och ISO/IEC 27001.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Äger denna policy och säkerställer att den är anpassad till det övergripande ISMS, riskhantering och organisationens strategi för regelefterlevnad.

4.1.2 Godkänner nivåer för leverantörsklassificering, resultat från säkerhetsgranskningar och undantag med hög risk.

4.1.3 Deltar vid eskalering av allvarliga leverantörsincidenter och i avtalsförhandlingar för kritiska tjänster.

4.2 Upphandling och leverantörsstyrning

4.2.1 Säkerställer att alla nya och förnyade leverantörsavtal innehåller godkända säkerhetsklausuler och dataskyddsklausuler.

4.2.2 Upprätthåller det centrala leverantörsregistret och samordnar med juridik- och regelefterlevnadsansvariga avseende dokumentation av tredjepartsrisker.

4.2.3 Initierar introduktionsprocesser och säkerställer anpassning till säkerhetsbedömningar före avtalstecknande.

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

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas minst årligen, eller tidigare vid:

9.1.1 Väsentliga förändringar i upphandlingsstrategin eller leverantörsekosystemet

9.1.2 Uppdateringar av rättsliga eller regulatoriska ramverk (t.ex. DORA-förordningen, EU:s GDPR)

9.1.3 Större incidenter hos tredje part, personuppgiftsincidenter eller revisionsbrister

9.1.4 Resultat från riskbedömningar eller externa certifieringsorgan

9.2 Granskningsprocessen ägs gemensamt av CISO, upphandling, juridik och riskhanteringsfunktionen.

9.3 Alla policyrevideringar ska dokumenteras i ISMS-registret för dokumentstyrning, versionshanteras och kommuniceras till relevanta intressenter via styrningskanaler för leverantörer och informationsinsatser.

9.4 Ersatta versioner ska arkiveras i minst tre år för spårbarhet och efterlevnad av rättsliga krav.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer det övergripande åtagandet att skydda all verksamhet i organisationen, inklusive beroenden av tredjepartsleverantörer och externa IT-tjänsteleverantörer.

10.2 P6 – Riskhanteringspolicy. Vägleder identifiering, bedömning och riskreducering av risker kopplade till tredjepartsrelationer, inklusive ärvda eller systemiska risker i leverantörsekosystemet.

10.3 P17 – Policy för dataskydd och integritet. Gäller för alla leverantörer som hanterar personuppgifter och kräver lämpliga avtalsvillkor, skyddsåtgärder för överföring och principer för inbyggt integritetsskydd.

10.4 P4 – Åtkomstkontrollpolicy. Styr hur tredjepartspersonal får åtkomst till organisationens system genom tillämpning av rollbaserade behörigheter, sessionsskydd och rutiner för återkallelse.

10.5 P22 – Loggnings- och övervakningspolicy. Kräver att leverantörers åtkomst till system övervakas, loggas och granskas, särskilt i miljöer där privilegierade eller datacentrerade aktiviteter förekommer.

10.6 P30 – Policy för incidenthantering. Definierar eskaleringsrutiner och krav på incidentrapportering för säkerhetshändelser som har sitt ursprung hos leverantörer eller vid gemensamma utredningar som omfattar tredjepartssystem.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001: Klausul 8.1 – Operativ planering och styrning: Kräver formella kontroller för tredjepartstjänster som påverkar ISMS.

11.2 ISO/IEC 27002:2022 – Kontroller 5.19 till 5.22:

11.2.1 Bilaga A, kontroll 5.19 – Policyer och rutiner för leverantörsrelationer: Kräver kontroller för att hantera interaktioner med leverantörer.

11.2.2 Bilaga A, kontroll 5.20 – Hantering av leverantörsrisker: Fokuserar på identifiering, bedömning och löpande tillsyn av leverantörers säkerhetsläge.

11.2.3 Bilaga A, kontroll 5.21 – Styrning av leverans av leverantörstjänster: Kräver att prestation och säkerhet är anpassade till avtalskraven.

11.2.4 Bilaga A, kontroll 5.22 – Övervakning och granskning av leverantörer: Förstärker behovet av löpande validering och omprövning av tredje parts efterlevnad.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Externa systemtjänster: Definierar säkerhets- och riskkrav för system som drivs av externa parter.

11.3.2 SA-10 – Utvecklares konfigurationshantering: Gäller när tredje part levererar programvara eller miljöer.

11.3.3 CA-3 – Systemsammanlänkningar: Kräver tillsyn och överenskommelse om dataflöden mellan parters system.

11.3.4 PS-7 – Personalsäkerhet för tredje part: Säkerställer att entreprenörer och leverantörspersonal granskas och följs upp på ett lämpligt sätt.

11.4 EU:s GDPR (2016/679):

11.4.1 Artikel 28 – Skyldigheter för personuppgiftsbiträden: Kräver skriftliga avtal med biträden som behandlar data, inklusive tekniska och organisatoriska åtgärder (TOM).

11.4.2 Artikel 32 – Säkerhet i behandlingen: Kräver lämpliga skyddsåtgärder för både personuppgiftsansvariga och personuppgiftsbiträden.

11.4.3 Artikel 33 – Anmälan av personuppgiftsincidenter: Kräver skyndsam avisering från leverantörer vid incidenter.

11.5 EU:s NIS2-direktiv (2022/2555):

11.5.1 Artikel 21.2 e–f: Kräver riskbaserad leverantörshantering och säkerhetstillsyn, särskilt i digitala leveranskedjor hos väsentliga och viktiga verksamhetsutövare.

11.6 EU:s DORA-förordning (2022/2554):

11.6.1 Artikel 28 – IKT-risker kopplade till tredje part: Ställer krav på riskbedömning, avtalsmässiga säkerhetsvillkor och exitstrategier för leverantörer av finansiella tjänster.

11.6.2 Artikel 30 – Tillsyn av kritiska IKT-tredjepartsleverantörer: Fastställer skärpta krav på övervakning och tillsyn för nyckelleverantörer.

11.7 COBIT 2019:

11.7.1 BAI05 – Hantera organisatorisk förändringsförmåga: Säkerställer att övergångar mellan leverantörer styrs på ett säkert sätt.

11.7.2 DSS02 – Hantera servicebegäranden och incidenter: Gäller leverantörsrapporterade problem och integration med incidenthantering.

11.7.3 MEA03 – Övervaka, utvärdera och bedöma regelefterlevnad: Förstärker mätning av leverantörsprestanda och övervakning av efterlevnad.