					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P26S					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	Operativa säkerhetsåtgärder för relationer med tredje part och leverantörer
ISO/IEC 27002:2022	Kontroller 5.19–5.22	Kontroller för leverantörssäkerhet, avtalsenliga säkerhetsvillkor, ändringshantering, övervakning och granskning
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Anskaffning, konfiguration, samtrafikavtal och kontroller för extern personal
EU:s GDPR	Artiklarna 28, 32	Personuppgiftsbiträdesavtal och säkerhetskrav för personuppgiftsbiträden
EU:s NIS2-direktiv	Artiklarna 21(2)(a)(b)(i), 23(1)	Riskhantering i leveranskedjan och tillsyn över tredjepartstjänster
DORA-förordningen	Artiklarna 5(1)(2), 28(1)(2)	IKT-riskhantering för tredjepartsleverantörer av IKT-tjänster
COBIT 2019	APO10, APO12, DSS05	Leverantörsstyrning och integrering av risker

1. Syfte

1.1 Denna policy fastställer obligatoriska säkerhetskrav för att ingå, hantera och avsluta relationer med tredje part och leverantörer som ges åtkomst till eller påverkar organisationens data, system eller tjänster.

1.2 Den säkerställer att externa leverantörer, inklusive IT-supportleverantörer, leverantörer av molntjänster, programvaruutvecklare och entreprenörer som stödjer verksamhetsprocesser, hanterar organisationens tillgångar på ett säkert sätt och i enlighet med tillämpliga lagkrav och standarder.

1.3 Denna policy minskar risker såsom dataläckage, obehöriga systemändringar, regulatoriska sanktionsavgifter och verksamhetsavbrott som orsakas av osäkra eller bristfälligt styrda tredjepartsarrangemang.

2. Omfattning

2.1 Denna policy gäller för alla tredje parter som:

2.1.1 Tillhandahåller programvara, infrastruktur, drift eller molntjänster

2.1.2 Ges åtkomst till eller hanterar interna system, enheter eller applikationer

2.1.3 Hanterar organisationens data, dokument eller säkerhetskopior

2.1.4 Stödjer verksamheten, HR, ekonomi eller kundtjänst

2.2 Den gäller även för:

2.2.1 Intern personal som deltar i urval, upphandling eller tillsyn av leverantörer

2.2.2 All personal som hanterar leverantörsintroduktion, avtal, åtkomst eller granskningar

2.2.3 Alla system eller processer som är beroende av komponenter eller tjänster från tredje part

3. Mål

3.1 Säkerställa att alla leverantörer uppfyller tydligt definierade säkerhetskrav.

3.2 Kräva att leverantörsavtal innehåller bindande avtalsvillkor avseende säkerhet, integritetsskydd och incidenthantering.

3.3 Bedöma och dokumentera leverantörsrisker innan avtal ingås eller åtkomst beviljas.

3.4 Tillämpa regelbundna granskningar av leverantörer med hög risk eller kritisk betydelse för att verifiera efterlevnad.

3.5 Etablera en formell process för undantag, incidenthantering och uppdatering av avtal.

3.6 Stödja efterlevnad av skyldigheter enligt ISO/IEC 27001:2022, EU:s GDPR, EU:s NIS2-direktiv och DORA-förordningen avseende leverantörsstyrning.

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Har det övergripande ansvaret för urval av leverantörer och efterlevnad av säkerhetskrav

4.1.2 Godkänner avtal, undantag och eskaleringar som rör leverantörer

4.1.3 Utövar tillsyn över incidenthantering och beslutsfattande när leverantörer inte uppfyller sina skyldigheter

4.2 IT-leverantör eller intern säkerhetsansvarig

4.2.1 Utvärderar den tekniska åtkomst som leverantörer begär

4.2.2 Inför åtkomstkontroller, granskar loggar och verifierar säker datahantering

4.2.3 Granskar underlag avseende säkerhetskontroller, certifieringar eller revisionsresultat, där så är tillämpligt

[... 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 av verkställande direktör, med deltagande från IT-leverantören eller leverantörsansvarig.

9.2 Policyn ska även granskas:

9.2.1 Efter varje väsentlig förändring i rättsliga, regulatoriska eller avtalsmässiga skyldigheter

9.2.2 Efter en leverantörsrelaterad säkerhetsincident eller revisionsiakttagelse

9.2.3 Vid införande av nya leverantörskategorier, till exempel kritiska SaaS-plattformar

9.3 Alla uppdateringar ska:

9.3.1 Dokumenteras med versionshistorik och motivering

9.3.2 Godkännas av verkställande direktör

9.3.3 Kommuniceras till relevant intern personal och leverantörsansvariga

9.3.4 Bevaras tillsammans med tidigare versioner enligt P14S – Policy för databevarande och bortskaffning

10. Relaterade policyer och kopplingar

10.1 Effektiviteten i denna policy är beroende av samordning med följande SME-policyer för informationssäkerhet:

10.1.1 P2S – Policy för styrningsroller och ansvar: Tilldelar ansvar för leverantörstillsyn och tillämpning av avtal.

10.1.2 P4S – Policy för åtkomstkontroll: Anger regler för åtkomstbegränsning som ska tillämpas när leverantörer ges systemåtkomst.

10.1.3 P17S – Policy för dataskydd och integritet: Säkerställer att leverantörer som hanterar personuppgifter följer dataskyddsprinciper och rättsliga krav.

10.1.4 P14S – Policy för databevarande och bortskaffning: Gäller för alla data eller uppgifter som delas med eller lagras av leverantörer och styr säker avveckling efter att avtal har upphört.

10.1.5 P30S – Policy för incidenthantering: Definierar hur organisationen ska agera när en leverantör orsakar eller är involverad i en säkerhetsincident, inklusive eskalering och rutiner för hantering av bevismaterial.

10.2 Dessa policyer samverkar för att säkerställa att leverantörsrisker hålls under kontroll under hela avtalets livscykel.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver införande av operativa säkerhetsåtgärder, inklusive sådana som tillämpas på relationer med tredje part och leverantörer.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.19 – Säkerställer att leverantörers säkerhetsåtgärder är anpassade till organisationens krav.

11.2.2 Kontroll 5.20 – Kräver formella avtal som omfattar säkerhetsvillkor, ansvar och skyldigheter vid överträdelser.

11.2.3 Kontroll 5.21 – Styr förändringar i leverantörstjänster som kan påverka säkerhetsläget.

11.2.4 Kontroll 5.22 – Kräver övervakning och granskning av leverantörstjänster och efterlevnad.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Reglerar anskaffning av externa system och tjänster och kräver riskbedömningar samt definierade krav.

11.3.2 SA-10 – Styr konfigurations- och ändringsrutiner som omfattar system som hanteras av tredje part.

11.3.3 CA-3 – Kräver samtrafikavtal för system som involverar externa parter.

11.3.4 PS-7 – Anger krav på kontroll och ansvar för extern personal.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 28 – Kräver personuppgiftsbiträdesavtal med leverantörer som agerar personuppgiftsbiträde.

11.4.2 Artikel 32 – Kräver lämpliga tekniska och organisatoriska säkerhetsåtgärder för alla personuppgiftsbiträden som behandlar data.

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

11.5.1 Artikel 21(2)(a), (b), (i) – Kräver IKT-riskhantering i leveranskedjan och kontroller för tredje part.

11.5.2 Artikel 23(1) – Kräver dokumenterad tillsyn över tredjepartstjänster för väsentliga och viktiga entiteter.

11.6 DORA-förordningen (2022/2554)

11.6.1 Artikel 5(1) – Kräver ett ramverk för IKT-riskhantering som omfattar alla kritiska tredjepartsleverantörer.

11.6.2 Artikel 5(2) – Fastställer avtalsmässiga och operativa kontroller för beroenden till IKT-tjänster.

11.6.3 Artikel 28(1), (2) – Fastställer regler för tillsyn över IKT-risker kopplade till tredje part inom finanssektorn.

11.7 COBIT 2019

11.7.1 APO10 – ”Manage Suppliers” beskriver kontroller för sourcing och förväntningar på relationshantering.

11.7.2 APO12 – ”Manage Risk” integrerar leverantörsrisk i organisationens riskstyrning.

11.7.3 DSS05 – ”Manage Security Services” gäller hanterade tredjepartstjänster och utkontrakterade tjänsteleverantörer.