					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P28S					Dokumenttitel: **Policy för outsourcad utveckling**							
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/förordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 5.1, 6.1, 8	Tillämpliga ISMS-kontroller och leverantörsrelaterade kontroller
ISO/IEC 27002:2022	Kontroller 5.19, 5.20, 8.25–8.27	Kontroller för leverantörer och säker utvecklingslivscykel
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Krav för anskaffning, leveranskedja, säker utveckling och leverantörsavtal
EU:s GDPR	Artikel 28	Avtalskrav och dataskyddskrav för behandling av personuppgifter av tredje part
EU:s NIS2-direktiv	Artikel 21(2)(a), (h)	Kontroller för leveranskedjan och säker applikationsutveckling
EU:s DORA-förordning	Artikel 10	IKT-riskhantering för tredje part, inklusive outsourcad utveckling
COBIT 2019	BAI03, DSS05	Krav för extern utveckling och externa IT-tjänsteleverantörer

1. Syfte

1.1 Denna policy säkerställer att all outsourcad programvaruutveckling, oavsett om den utförs av frilansare, byråer eller tredjepartsleverantörer, genomförs på ett säkert sätt, omfattas av avtalsmässig styrning och är anpassad till tillämpliga rättsliga, regulatoriska och revisionsrelaterade krav.

1.2 Policyn skyddar organisationen mot risker kopplade till osäker kod, otydligt ägarskap, dataexponering och bristfällig leverantörsstyrning genom att ställa krav på bindande utvecklingsstandarder och tillsyn över leverantörer, även när en särskild IT-avdelning saknas.

1.3 Denna policy stödjer certifiering enligt ISO/IEC 27001:2022 genom att fastställa tydliga krav för utveckling, ansvar och dokumenterade kontroller för utvecklingsaktiviteter som utförs av tredje part.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla externa utvecklare, inklusive frilansare och utvecklingsbyråer

2.1.2 Allt utvecklingsarbete som omfattar interna verktyg, publika webbplatser, programvaruapplikationer eller verksamhetsautomatisering

2.1.3 Personal som ansvarar för att välja, hantera eller utöva tillsyn över externa utvecklare

2.1.4 All systemintegration, skriptutveckling eller annan utveckling som utförs av tredje part och som interagerar med företagets data eller system

2.2 Den omfattar även varje part eller plattform som har åtkomst till företagets autentiseringsuppgifter, datalagringsplatser, källkodslager, testmiljöer eller produktionssystem.

3. Mål

3.1 Säkerställa att all outsourcad utveckling följer principer för säker kodning och att utvecklare genom avtal är skyldiga att följa dokumenterade standarder och sekretessklausuler.

3.2 Fastställa ägarskap för alla leverabler, inklusive kod, tillgångar, autentiseringsuppgifter och dokumentation, så att en fullständig överföring av rättigheter till företaget säkerställs och överlämningen vid projektavslut sker på ett spårbart sätt.

3.3 Förebygga vanliga utvecklingsrisker, inklusive återanvändning av proprietär kod, angrepp via leveranskedjan genom bibliotek, användning av ramverk som inte längre stöds samt administrativ åtkomst som inte har granskats.

3.4 Kräva dokumentation före uppdragets start för varje outsourcat projekt, inklusive avtal, sekretessavtal (NDA) och lägsta säkerhetskrav.

3.5 Skydda kunddata, system och interna processer genom att kräva stark tillsyn över utvecklingen, testning efter leverans och säker hantering av systemåtkomst.

4. Roller och ansvar

4.1 Verkställande chef (GM)

4.1.1 Godkänner alla leverantörsrelationer och undertecknar utvecklingsavtal.

4.1.2 Säkerställer att all outsourcad utveckling följer denna policy.

4.1.3 Återkallar åtkomst till företagets system när projektet har avslutats.

4.1.4 Granskar dokumentation och leveransresultat efter slutförd leverans.

4.2 Projektägare (vanligtvis en intern medarbetare eller utsedd samordnare)

4.2.1 Ansvarar för den dagliga samordningen med den externa utvecklaren.

4.2.2 Verifierar att funktionella krav uppfylls och att leverabler testas.

4.2.3 Säkerställer säker överlämning av kod och autentiseringsuppgifter.

4.2.4 Rapporterar utvecklingsrelaterade problem eller incidenter till GM.

[... 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 Årlig granskning

9.1.1 Denna policy ska granskas av verkställande chef (GM) minst en gång per år. Granskningen ska säkerställa att policyn fortsatt uppfyller:

9.1.1.1 Krav för certifiering enligt ISO/IEC 27001

9.1.1.2 Ändringar i rättsliga skyldigheter, till exempel artikel 28 i EU:s GDPR och artikel 10 i DORA-förordningen

9.1.1.3 Aktuella utvecklingsmetoder på SME-nivå och tredjepartsrisker

9.2 Extra granskningar

9.2.1 Policygranskningar ska också genomföras när:

9.2.1.1 En ny leverantör eller plattform för outsourcad utveckling introduceras

9.2.1.2 En väsentlig incident som rör outsourcad utveckling inträffar

9.2.1.3 Det sker väsentliga ändringar i använda verktyg, plattformar eller miljöer

9.3 Granskningsprocess

9.3.1 GM ansvarar för att:

9.3.1.1 Verifiera att avtal, sekretessavtal (NDA) och processer för åtkomstkontroll fortsatt är effektiva

9.3.1.2 Bekräfta att nuvarande leverantörer och frilansare följer policyn

9.3.1.3 Revidera kraven utifrån återkoppling från tidigare projekt eller incidenter

9.4 Versionshantering och kommunikation

9.4.1 Alla ändringar ska:

9.4.1.1 Registreras med datum, orsak och beskrivning av ändringen

9.4.1.2 Godkännas av GM och läggas till i versionshistoriken

9.4.1.3 Kommuniceras till all personal eller projektägare som arbetar med externa utvecklare

9.4.1.4 Distribueras på nytt till alla berörda leverantörer och tredje parter där det är nödvändigt

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer direkt och är beroende av genomförandet av följande SME-anpassade policyer:

10.1.1 P2S – Policy för styrningsroller och ansvar: Förtydligar vem som ansvarar för leverantörsgodkännande, åtkomstkontroll och riskacceptans vid användning av externa utvecklare.

10.1.2 P4S – Policy för åtkomstkontroll: Definierar korrekt skapande, begränsning och avslut av användarkonton och administrativ åtkomst som används vid outsourcad utveckling.

10.1.3 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att intern personal förstår hur samordning med externa utvecklare ska ske på ett säkert sätt, inklusive hantering av autentiseringsuppgifter och projektfiler.

10.1.4 P17S – Policy för dataskydd och integritet: Fastställer säkerhetskrav och rättsliga krav för hantering av personuppgifter som kan behandlas av externa utvecklare enligt EU:s GDPR.

10.1.5 P24S – Policy för säker utveckling: Anger hur intern och extern utveckling ska följa praxis för säker kodning samt granskning av bibliotek och ramverk.

10.1.6 P30S – Policy för incidenthantering: Krävs när outsourcad utveckling leder till säkerhetsincidenter eller sårbarheter och styr samordnad utredning och korrigerande åtgärder.

10.2 Dessa policyer ska genomföras parallellt för att säkerställa att outsourcad utveckling inte skapar ohanterad risk eller leder till bristande efterlevnad av SME-relaterade krav.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Organisationer ska bedöma och hantera informationssäkerhetsrisker kopplade till leverantörer.

11.1.2 Klausul 8.1 – Kräver operativ planering och styrning, inklusive tredjepartstjänster såsom outsourcad utveckling.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.19 – Rekommenderar att leverantörers förmåga att uppfylla informationssäkerhetskrav utvärderas.

11.2.2 Kontroll 5.20 – Rekommenderar regelbunden övervakning och periodisk granskning av tjänster från tredje part.

11.2.3 Kontroller 8.25–8.27 – Beskriver praxis för säker utvecklingslivscykel som är tillämplig på outsourcad utveckling.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Kräver att strategier för anskaffning omfattar informationssäkerhetsåtgärder.

11.3.2 SA-9 – Behandlar extern systemutveckling och risker i leveranskedjan.

11.3.3 SA-11 – Definierar säker utvecklingspraxis, inklusive kodgranskningar och åtgärdande av brister.

11.3.4 SA-15 – Rekommenderar automatiserade verktyg för att upptäcka brister och säkerställa programvara.

11.3.5 SR-3 – Kräver att leverantörsavtal omfattar cybersäkerhetskrav.

11.4 Europeiska unionens allmänna dataskyddsförordning (GDPR)

11.4.1 Artikel 28 – Kräver att avtal med personuppgiftsbiträden säkerställer lämpliga skyddsåtgärder för dataskydd, vilket är direkt tillämpligt på utvecklare som behandlar eller har åtkomst till personuppgifter.

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

11.5.1 Artikel 21(2)(a), (h) – Kräver säkerhetskontroller för leveranskedjan och säker programvaruutveckling för omfattade leverantörer av digitala tjänster, inklusive SME där så är tillämpligt.

11.6 EU:s DORA-förordning

11.6.1 Artikel 10 – Kräver IKT-riskhantering för tredje part, inklusive utvecklingsavtal, säkerhetsskyldigheter och riskkontroller relaterade till tredjepartsleverantörer.

11.7 COBIT 2019

11.7.1 BAI03 – Hantera identifiering och utveckling av lösningar – Säkerställer att extern utveckling uppfyller verksamhetskrav och säkerhetsförväntningar.

11.7.2 DSS05 – Hantera säkerhetstjänster – Kräver att externa säkerhetstjänster och utvecklingsleverantörer omfattas av tillämpade säkerhetsregler och står under tillsyn.