					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P28					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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8.1	Ej tillämpligt
ISO/IEC 27002:2022	Kontroller 5.19-5.22, 8	Ej tillämpligt
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	Ej tillämpligt
EU:s GDPR	Artiklarna 28, 32	Ej tillämpligt
EU:s NIS2-direktiv	Artiklarna 21(2)(a), (h), 23	Ej tillämpligt
EU:s DORA-förordning	Artiklarna 28(1), (2)	Ej tillämpligt
COBIT 2019	APO10, BAI03, DSS	Ej tillämpligt

1. Syfte

1.1 Denna policy fastställer obligatoriska kontroller för outsourcing av programvaru- eller systemutveckling till externa leverantörer, konsulter eller byråer för att säkerställa att säkra arbetssätt är integrerade genom hela utvecklingslivscykeln.

1.2 Policyn syftar till att förebygga säkerhetssårbarheter, dataförlust, exponering av immateriella rättigheter (IP) och brister i regelefterlevnad som kan uppstå vid extern utveckling.

1.3 Policyn fastställer krav på leverantörsstyrning, säker kodningspraxis, identitets- och åtkomsthantering, övervakning samt avveckling av uppdrag vid avtalets upphörande för att upprätthålla konfidentialitet, riktighet och tillgänglighet i utvecklad programvara.

2. Omfattning

2.1 Denna policy gäller för samtliga organisatoriska enheter som anlitar externa parter för programvaru- eller systemutveckling, inklusive:

2.1.1 webbapplikationer, mobilappar, inbyggda system, API:er, skript, automatiserade arbetsflöden eller plattformsmoduler

2.1.2 kundanpassad utveckling för interna plattformar, kundvända system eller kommersiella produkter

2.1.3 uppdrag med tredjepartsutvecklare, frilansare, byråer eller offshoreteam

2.2 Policyn gäller även för varje extern part som under utvecklingen får åtkomst till källkod, testmiljöer eller CI/CD-pipelines.

2.3 Kraven är bindande oavsett avtalstyp, utvecklingsmetodik eller geografisk placering för den outsourcade leverantören.

3. Mål

3.1 Säkerställa att arbetssätt för säker utvecklingslivscykel (SDLC) tillämpas i alla outsourcade uppdrag, från planering till validering efter driftsättning.

3.2 Säkerställa att alla avtal med externa utvecklare innehåller obligatoriska klausuler om dataskydd, säker kodning och bibehållet ägande av immateriella rättigheter.

3.3 Fastställa krav på åtkomstkontroll, övervakning och revision för tredjepartsutvecklare som interagerar med interna system.

3.4 Skydda organisationen mot risker i leveranskedjan, rättsliga överträdelser och anseendeskada kopplade till externt utvecklad programvara.

3.5 Upprätthålla löpande efterlevnad av säkerhetsramverk och regelverk, inklusive ISO/IEC 27001, NIST, GDPR, NIS2, DORA och COBIT 2019.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner outsourcade utvecklingsprojekt med hög risk och beslutar om policyundantag när detta är motiverat.

4.1.2 Säkerställer att beslut om outsourcing är i linje med strategiska mål och organisationens riskaptit.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Godkänner onboarding av leverantörer ur ett säkerhetsperspektiv.

4.2.2 Fastställer krav på säkerhetskontroller för outsourcade uppdrag och granskar incidentrapporter.

[... 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 en gång per år eller oftare under följande omständigheter:

9.1.1 införande av nya modeller, leverantörer eller jurisdiktioner för outsourcad utveckling

9.1.2 uppdateringar av regelverk såsom GDPR, NIS2 eller DORA

9.1.3 efter en säkerhetsincident som rör outsourcad kod, åtkomst eller leveranser

9.1.4 som en del av interna revisionsiakttagelser eller förbättringar av ISMS

9.2 Informationssäkerhetschef (CISO) ansvarar för att initiera och samordna policygranskningen i samråd med:

9.2.1.1 Juridik och Upphandling (för anpassning till avtalsmässig tillämpning)

9.2.1.2 projektägare och produktägare (för operativ genomförbarhet)

9.2.1.3 Informationssäkerhetsfunktionen (för uppdateringar av hot och kontroller)

9.2.1.4 Verkställande ledning (för slutligt godkännande)

9.3 Alla policyuppdateringar ska:

9.3.1.1 versionshanteras och lagras i ett utsett dokumentarkiv

9.3.1.2 kommuniceras till intressenter som deltar i outsourcad utveckling

9.3.1.3 kopplas till uppdateringar i relaterade policyer eller procedurdokumentation

9.4 En ändringslogg ska följa varje policyversion för att säkerställa spårbarhet av ändringar och godkännanden.

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer och stöds av följande relaterade dokument:

10.1.1 P1 - Informationssäkerhetspolicy: Fastställer säkerhetsprinciper på organisationsnivå som gäller i både interna och externa utvecklingssammanhang.

10.1.2 P5 - Ändringshanteringspolicy: Säkerställer att alla ändringar kopplade till driftsättning från outsourcade kodbaser granskas och godkänns före genomförande.

10.1.3 P13 - Policy för dataklassificering och märkning: Fastställer hur känsliga data ska identifieras innan de exponeras för utvecklingsleverantörer eller kodlager.

10.1.4 P18 - Policy för kryptografiska kontroller: Styr hur nycklar, hemligheter och känsliga åtkomstuppgifter ska hanteras under utveckling och leverans.

10.1.5 P24 - Policy för säker utveckling: Fastställer baslinjekrav för intern och extern programvaruutveckling.

10.1.6 P30 - Policy för incidenthantering: Styr hur överträdelser eller säkerhetsproblem som rör outsourcad utveckling ska eskaleras, utredas och hanteras.

10.1.7 P33 - Policy för övervakning, revision och regelefterlevnad: Fastställer krav för granskning av aktiviteter inom outsourcad utveckling vid revisioner eller efterlevnadsgranskningar.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända säkerhetsramverk och regelverk för att säkerställa säker outsourcing av programvaruutveckling och ändamålsenlig leverantörsstyrning.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 - Operativ planering och styrning: Fastställer processkontroller för säker utveckling och säker leverans från tredje part.

11.3 ISO/IEC 27002:2022 - Kontroller 5.19 till 5.21, 8.

11.3.1 Bilaga A Kontroll 5.19 - Hantering av leverantörsrelationer: Kräver formella avtal med klausuler om säkerhet och regelefterlevnad.

11.3.2 Bilaga A Kontroll 5.20 - Hantering av informationssäkerhet i leverantörsavtal: Säkerställer att utvecklingsspecifika kontroller byggs in i avtal.

11.3.3 Bilaga A Kontroll 5.21 - Hantering av leverantörers tjänsteleverans: Omfattar övervakning av leveranser och risker i tredjepartsutveckling.

11.3.4 Bilaga A Kontroll 8.27 - Outsourcad utveckling: Kräver definierade säkerhetskrav och åtkomstkontroll för programvara som utvecklas externt.

11.3.5 Dessa kontroller fastställer strukturerade krav för urval, avtalstecknande och tillsyn av outsourcade utvecklare, inklusive säker utvecklingspraxis, kodhantering och validering av leveranser.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Anskaffning: Kräver att krav på säker utveckling definieras vid anskaffningstillfället.

11.4.2 SA-9 - Externa systemtjänster: Styr hur tredjepartsutvecklare på ett säkert sätt får interagera med interna tjänster.

11.4.3 SA-10 - Utvecklarens konfigurationshantering: Överensstämmer med krav på versionshantering, kodåtkomst och ändringsspårning för externa team.

11.5 EU:s GDPR (2016/679)

11.5.1 Artikel 28 - personuppgiftsbiträdets skyldigheter: Kräver att avtal med tredjepartsutvecklare specificerar krav på säkerhet, kontroll och revision vid behandling av personuppgifter.

11.5.2 Artikel 32 - säkerhet i behandlingen: Kräver lämpliga skyddsåtgärder (t.ex. kryptering, åtkomstkontroll) vid utveckling av system som behandlar personuppgifter.

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

11.6.1 Artiklarna 21(2)(a), (h), 23: Kräver att säker utvecklingspraxis tillämpas i tredjepartsuppdrag och digitala leveranskedjor, med tillsyn och teknisk verifiering.

11.7 EU:s DORA-förordning (2022/2554)

11.7.1 Artiklarna 28(1), (2): Kräver att finansiella entiteter hanterar tredjepartsrisker inom IKT genom avtalsmässiga kontroller och tillsyn över säker utveckling, särskilt vid kritisk outsourcad utveckling.

11.8 COBIT 2019

11.8.1 APO10 - Hantera leverantörer: Fastställer strukturerade krav för leverantörsutvärdering, avtal och övervakning av prestation.

11.8.2 BAI03 - Hantera lösningsutveckling: Mappas direkt mot säkra SDLC-processer, kodgranskningar och validering av utveckling.

11.8.3 DSS05 - Hantera säkerhetstjänster: Överensstämmer med övervakning och skydd av system som utvecklas externt eller av tredje part.