					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P24S					Dokumenttitel: **Policy för säker 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	Relevanta säkerhetsåtgärder för operativa arbetssätt, inklusive säker utveckling
ISO/IEC 27002:2022	Kontroller 8.25–8.27	Omfattar säker programvaruutvecklingslivscykel, testning och säkerhetsansvar för tredjepartsutvecklare
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Omfattar säker SDLC, åtkomstkontroll och hantering av sårbarheter i utveckling
EU:s GDPR	Artikel 25	Kräver inbyggt dataskydd och dataskydd som standard vid programvaruutveckling
EU:s NIS2-direktiv	Artikel 21(2)(a), (e), (h)	Kräver policyer för säker utveckling, styrning av användning av öppen källkod samt dokumentation av riskreducerande åtgärder
DORA-förordningen	Artiklar 6(7), 9(1)(c), 10(2)(c)	Säkerhet genom hela livscykeln för kritiska IKT-system inom finanssektorn
COBIT 2019	BAI	Ramverk för strukturerad, spårbar och resilient styrning av säker utveckling

1. Syfte

1.1 Denna policy säkerställer att all programvara, alla skript och alla webbaserade verktyg som utvecklas eller ändras av organisationen eller dess externa partner utvecklas på ett säkert sätt, så att risken för sårbarheter, obehörig åtkomst till data eller driftstörningar minimeras.

1.2 Den fastställer bindande krav för säker utveckling och säker kodningspraxis som ska följas av alla interna utvecklare, uppdragstagare och leverantörer, oavsett projektets storlek eller komplexitet.

1.3 Denna policy syftar till att skydda kunddata, förebygga incidenter och säkerställa att programvara som utvecklas eller anpassas av eller för organisationen kan genomgå säkerhetsrevisioner, uppfylla rättsliga krav (t.ex. GDPR, NIS2 och DORA) och stödja certifiering enligt ISO/IEC 27001.

2. Omfattning

2.1 Denna policy gäller för alla personer och enheter som på organisationens uppdrag deltar i utveckling, anpassning, driftsättning eller förvaltning av följande:

2.1.1 Webbplatser, applikationer eller automatiseringsverktyg

2.1.2 Internt utvecklade skript eller programvaror

2.1.3 Kod som utvecklats av tredjepartsutvecklare eller frilansare

2.1.4 Insticksprogram, bibliotek och programvarukomponenter som integreras i produktionssystem

2.2 Den omfattar alla miljöer som används i utvecklingsaktiviteter, inklusive:

2.2.1 Utvecklings- och testmiljöer

2.2.2 Staging- och förproduktionsmiljöer

2.2.3 Produktionssystem som används för att köra egenutvecklad kod

2.3 Policyn reglerar även hantering av data vid utveckling och driftsättning, särskilt all användning av produktionsdata i icke-produktionsmiljöer.

3. Mål

3.1 Att förhindra att säkerhetsbrister eller sårbarheter införs i egenutvecklad programvara eller programvara som utvecklats av tredje part.

3.2 Att säkerställa att säker kodningspraxis och förebyggande av sårbarheter integreras i varje fas av programvarans livscykel.

3.3 Att minska risker kopplade till användning av öppen källkod eller tredjepartskomponenter genom att kräva korrekt granskning och spårbarhet.

3.4 Att kräva formell kodgranskning och säkerhetstestning av applikationer före release.

3.5 Att styra åtkomst till utvecklingsmiljöer och säkerställa åtskillnad från produktionssystem.

3.6 Att uppfylla tillämpliga krav enligt internationella standarder och regelverk (t.ex. ISO/IEC 27001, GDPR, DORA och NIS2).

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Godkänner denna policy och är policyägare.

4.1.2 Säkerställer att all programvaruutveckling, intern eller utkontrakterad, följer denna policy.

4.1.3 Granskar och undertecknar utvecklingsavtal eller tjänsteavtal som innehåller klausuler om säker utveckling.

4.1.4 Verifierar leverantörers efterlevnad genom regelbundna avstämningar eller genom att begära säkerhetsunderlag.

4.2 Intern utvecklare eller applikationsägare

4.2.1 Följer säker kodningspraxis och säkra driftsättningsrutiner.

4.2.2 Tillämpar checklista för säker utveckling i varje projekt.

4.2.3 Validerar säkerheten i all öppen källkod och alla tredjepartskomponenter som används.

4.2.4 Rapporterar omedelbart alla identifierade sårbarheter till VD.

[... 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 av verkställande direktör minst en gång per år för att:

9.1.1 Verifiera fortsatt efterlevnad av ISO/IEC 27001, GDPR, NIS2 och DORA

9.1.2 Återspegla uppdaterade hot eller förändringar i bästa praxis för säker utveckling

9.1.3 Säkerställa kompatibilitet med nya verktyg, plattformar eller leverantörsrelationer

9.2 Extra granskningar ska initieras vid:

9.2.1 Alla rapporterade säkerhetsincidenter relaterade till programvara

9.2.2 Införande av nytt utvecklingsramverk eller ny driftplattform

9.2.3 Byte av tredjepartsleverantör för utveckling

9.2.4 Regulatoriska uppdateringar som påverkar programvara eller säkerhetsrelaterade skyldigheter

9.3 Alla ändringar i denna policy ska:

9.3.1 Dokumenteras med datum, ändringssammanfattning och VD:s godkännande

9.3.2 Kommuniceras tydligt till all intern och extern utvecklingspersonal

9.3.3 Sparas som en del av organisationens versionshantering och ändringshistorik för policyer

9.4 Uppdaterade versioner ska vara lätt tillgängliga, antingen via interna plattformar, tryckt dokumentation eller molntjänster som är tillgängliga för leverantörer.

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer och är beroende av ett effektivt genomförande av flera andra SME-policyer:

10.1.1 P2S – Policy för styrningsroller och ansvar: Fastställer ansvar för tilldelning och verifiering av säkerhetskontroller för utveckling i projekt och hos leverantörer.

10.1.2 P4S – Policy för åtkomstkontroll: Anger grundläggande regler för att begränsa åtkomst till utvecklingsmiljöer och kodlagringsplatser, inklusive funktionsseparering.

10.1.3 P8S – Policy för medvetenhet och utbildning inom informationssäkerhet: Säkerställer att interna utvecklare och uppdragstagare förstår säker kodningspraxis och tillhörande säkerhetsansvar.

10.1.4 P17S – Policy för dataskydd och integritet: Klargör hur personuppgifter ska hanteras vid utveckling, testning och loggning för att uppfylla GDPR.

10.1.5 P30S – Policy för incidenthantering: Definierar hur utvecklingsrelaterade säkerhetsincidenter ska rapporteras, bedömas och hanteras, inklusive kodrelaterade exponeringar.

10.2 Dessa policyer samverkar för att säkerställa att säker utveckling är genomförbar och granskningsbar, även i en liten eller icke-teknisk organisation.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver att operativa kontroller, inklusive säker utveckling, införs i linje med verksamhetsmål och risknivå.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – Rekommenderar att säkerhet integreras genom hela programvarans livscykel, inklusive källkodshantering, versionshantering och utvecklaråtkomst.

11.2.2 Kontroll 8.26 – Anger metoder för applikationstestning och verifiering av säkerhetsfunktionalitet före driftsättning.

11.2.3 Kontroll 8.27 – Kräver att tredjepartsutvecklare följer samma utvecklingsstandarder och att deras säkerhetsansvar är tydligt definierat.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 till SA-15 – Definierar processer för säker utveckling, inklusive åtkomstkontroll för utvecklare, testning, hotmodellering och dokumentation.

11.3.2 SI-10 – Kräver att utvecklare identifierar och reducerar vanliga programvarusvagheter samt använder automatiserade verktyg där det är tillämpligt.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 25 – ”Inbyggt dataskydd och dataskydd som standard” kräver att säkerhets- och integritetsskydd integreras i programvarans design och utveckling, särskilt där personuppgifter behandlas.

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

11.5.1 Artikel 21(2)(a), (e) och (h) – Kräver policyer för säker utveckling, styrning av användning av öppen källkod samt dokumenterad riskreducering för applikationsrelaterade risker i väsentliga och viktiga entiteter.

11.6 DORA-förordningen (2022/2554)

11.6.1 Artiklarna 6(7), 9(1)(c) och 10(2)(c) – Fastställer säkerhetskrav för utvecklingslivscykeln för entiteter i finanssektorn, inklusive SME-företag, särskilt för kritiska IKT-system.

11.7 COBIT 2019

11.7.1 BAI03 – ”Manage Solutions Identification and Build” stödjer införandet av strukturerade utvecklingskontroller som betonar säkerhet, spårbarhet och resiliens, anpassade till SME-begränsningar.