					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P24					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**

1. Syfte

1.1 Denna policy fastställer obligatoriska säkerhetskrav för aktiviteter inom programvaru- och systemutveckling i organisationen, inklusive interna projekt, outsourcad utveckling och integration av kod från tredje part.

1.2 Syftet är att säkerställa att säkerhet byggs in genom hela livscykeln för programvaruutveckling (SDLC) och att sårbarheter identifieras, riskreduceras och förebyggs före driftsättning i produktion.

1.3 Denna policy stödjer tillämpningen av ISO/IEC 27001:2022 klausul 8.1 och bilaga A, kontrollerna 8.25–8.28, genom att standardisera styrningen av säker utveckling, praxis för kodvalidering och tillsyn över utveckling som utförs av tredje part.

2. Omfattning

2.1 Denna policy gäller för all:

2.1.1 Programvara, applikationer, skript, integrationer och automatiseringsverktyg som utvecklas internt eller externt.

2.1.2 Utvecklingsteam, produktägare, DevOps, QA, arkitekter, projektledare och konsulter.

2.1.3 SDLC-miljöer, inklusive utvecklings-, test-, staging- och förproduktionsmiljöer.

2.1.4 Komponenter med öppen källkod och komponenter från tredje part som integreras i interna applikationer.

2.1.5 Programvara som driftsätts lokalt, i privata molnmiljöer, hybrida miljöer eller publika molnmiljöer.

2.2 Alla användare och enheter som deltar i systemutveckling, testning eller driftsättning inom organisationens verksamhet omfattas av denna policy, inklusive leverantörer av hanterade tjänster och plattformsleverantörer.

3. Mål

3.1 Säkerhetskontroller ska byggas in i alla faser av programvaruutvecklingen, från design till driftsättning, så att riskreducering sker proaktivt och kontinuerligt.

3.2 Införande av exploaterbara sårbarheter, såsom injektionsbrister, osäker autentisering och exponering mot kända svagheter i komponenter från tredje part, ska förhindras.

3.3 Säker kodningspraxis i enlighet med OWASP, SANS CWE och ramverksspecifika riktlinjer ska fastställas och tillämpas.

3.4 All kod ska genomgå kollegial granskning, automatiserad analys och säkerhetsvalidering före driftsättning.

3.5 Utvecklingsrisker som uppstår till följd av outsourcade aktiviteter, integration av kod från tredje part och återanvändning av programvara med öppen källkod ska hanteras.

3.6 Utvecklings-, test- och stagingmiljöer ska skyddas mot obehörig åtkomst, och användning av produktionsdata utan godkänd datamaskering eller anonymisering ska förhindras.

3.7 Säkerhetsmedvetenheten hos utvecklare, produktägare och kvalitetsansvariga ska stärkas genom rollbaserad utbildning och löpande uppdateringar om framväxande hot.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Ansvarar för denna policy och säkerställer att kraven på säker utveckling tillämpas i hela organisationen.

4.1.2 Godkänner standarder för säker kodning och avtal avseende utveckling som utförs av tredje part.

4.1.3 Validerar beslut om riskbehandling för olösta eller uppskjutna sårbarheter.

4.2 Ansvarig för applikationssäkerhet / chef för DevSecOps

4.2.1 Tar fram, underhåller och förankrar riktlinjer för säker kodning.

4.2.2 Integrerar statisk och dynamisk säkerhetstestning i CI/CD-pipelines.

4.2.3 Genomför säkerhetsgranskningar av kod och fastställer obligatoriska korrigerande åtgärder.

[... 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 årligen, eller oftare som svar på:

9.1.1 Större förändringar i utvecklingsmetoder eller DevOps-verktyg.

9.1.2 Väsentliga säkerhetsincidenter som härrör från applikationssårbarheter.

9.1.3 Förändringar i regulatoriska krav kopplade till säker programvara (t.ex. GDPR, DORA).

9.1.4 Nya branschstandarder eller hotinformation (t.ex. OWASP Top 10, SLSA, MITRE CWE).

9.2 Granskning av policyn ska ledas av ansvarig för applikationssäkerhet i samordning med informationssäkerhetschefen (CISO), programvaruarkitekter, QA-ledning och juridisk rådgivare (för konsekvenser kopplade till kod från tredje part).

9.3 Alla revideringar ska registreras i ISMS-registret för dokumentstyrning, versionshanteras och kommuniceras till berörda team via versionsmeddelanden eller obligatorisk utbildning.

9.4 Äldre versioner ska bevaras i arkivlagringsplatsen för att säkerställa rättslig spårbarhet och revisionsspår.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer det strategiska mandatet för att bygga in säkerhet i alla organisationens informationssystem, där säker utveckling utgör en grundläggande operativ kontroll.

10.2 P4 – Policy för åtkomstkontroll. Definierar kontrollåtgärder för att begränsa åtkomst till utvecklingsmiljöer, kodlagringsplatser, byggverktyg och CI/CD-pipelines.

10.3 P5 – Ändringshanteringspolicy. Säkerställer att kodändringar, releaser och driftsättningar omfattas av korrekt godkännande, planering för återställning och verifiering efter driftsättning.

10.4 P12 – Policy för tillgångshantering. Stödjer inventering av utvecklingsmiljöer, källkodslagringsplatser och byggsystem som hanterade tillgångar som omfattas av klassificering och skydd.

10.5 P22 – Policy för loggning och övervakning. Gäller för utvecklingspipelines och säkerställer att byggprocesser, kodöverföringar och driftsättningshändelser loggas, övervakas och analyseras avseende säkerhetsavvikelser.

10.6 P30 – Policy för incidenthantering. Tillhandahåller ramverket för analys och hantering av säkerhetsbrister som upptäcks efter driftsättning eller under säkerhetstestning av applikationer.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Operativ planering och styrning: Kräver att processer och kontroller för säker utveckling integreras i verksamheten.

11.2 ISO/IEC 27002:2022 – Kontroller 8.25–8.28

11.2.1 Bilaga A kontroll 8.25 – Säker utvecklingslivscykel: Kräver att säkerhet formellt inkluderas i programvarudesign och utveckling.

11.2.2 Bilaga A kontroll 8.26 – Säkerhetskrav för applikationer: Kräver att säker kodning och säkerhetsrelaterade acceptanskriterier definieras.

11.2.3 Bilaga A kontroll 8.27 – Principer för säker systemarkitektur och utveckling: Kräver tillämpning av principer för säker design och hantering av kända svagheter.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 till SA-15: Etablerar strukturerad praxis för säker applikationsutveckling, inklusive krav på design, kodintegritet och testning.

11.3.2 SI-10 – Validering av informationsindata: Omfattar skydd genom säker kodningspraxis.

11.3.3 SR-3 – Skydd av leveranskedjan: Kräver granskning av programvara, komponenter och utvecklingsleverantörer från tredje part.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 25 – Inbyggt dataskydd och dataskydd som standard: Kräver att säkerhet och integritet byggs in i systemutvecklingen.

11.4.2 Artikel 32 – Säkerhet i behandlingen: Stödjer tekniska åtgärder såsom inmatningsvalidering, åtkomstkontroller och säker driftsättning.

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

11.5.1 Artikel 21(2)(e–f): Kräver metoder för programvaruutveckling som omfattar hantering av sårbarheter, kodsäkerhet och incidentrapportering.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Kräver praxis för säker utveckling för finansiella entiteter, inklusive kontroller för programvarukvalitet och åtgärdande av brister.

11.6.2 Artikel 10 – Verksamhetskontinuitet och testning: Främjar rigorös testning och validering av IKT-system, inklusive applikationer.

11.7 COBIT 2019

11.7.1 BAI03 – Hantera identifiering och utveckling av lösningar: Styr design, utveckling och integration av säkerhet i nya lösningar.

11.7.2 BAI07 – Hantera ändringsacceptans och övergång: Säkerställer säker driftsättning och utvärdering efter driftsättning.

11.7.3 DSS05 – Hantera säkerhetstjänster: Tillämpar säkerhetsvalidering på programvara och tjänsteleverans.