					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P25					Dokumenttitel: **Policy för säkerhetskrav för applikationer**							
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	—
ISO/IEC 27002:2022	Kontroller 8.25–8.28	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EU:s GDPR	Artiklarna 25, 32	—
EU:s NIS2-direktiv	Artiklarna 21.2 f, 23	—
DORA-förordningen	Artiklarna 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Syfte

1.1 Denna policy fastställer obligatoriska säkerhetskrav på applikationsnivå för programvara som utvecklas, anskaffas, integreras eller driftsätts av organisationen. Policyn säkerställer att alla applikationer utformas, implementeras och underhålls i enlighet med principer för säker utveckling, regulatoriska skyldigheter och organisationens riskaptit.

1.2 Policyn kräver att säkerhet integreras genom hela applikationens livscykel och omfattar användarautentisering, datahantering, skydd av gränssnitt samt säker interaktion med API:er och tjänster.

1.3 Genom att tillämpa denna policy ska organisationen förebygga att programvarusårbarheter införs, skydda känsliga data samt säkerställa spårbarhet och motståndskraft mot utnyttjande och missbruk.

2. Omfattning

2.1 Denna policy gäller för alla:

2.1.1 Internt utvecklade eller externt anskaffade applikationer, inklusive SaaS-tjänster och specialutvecklade verktyg

2.1.2 Applikationer som stödjer kritiska verksamhetsprocesser, kundåtkomst eller behandling av reglerade data

2.1.3 Utvecklings-, DevOps-, QA-, produkt- och säkerhetsteam

2.1.4 Tredjepartsutvecklare, programvaruleverantörer och integrationspartner med åtkomst till organisationens applikationer eller API:er

2.2 Policyn gäller i alla miljöer: utveckling, test, staging, produktion och katastrofåterställning, oavsett om de drivs lokalt, i privata datacenter eller i publika molnmiljöer.

3. Mål

3.1 Fastställa grundläggande funktionella och icke-funktionella säkerhetskrav som ska uppfyllas av alla applikationer, oavsett utvecklingsmetod eller teknikstack.

3.2 Säkerställa att skyddsåtgärder på applikationsnivå integreras, inklusive indatavalidering, kodning av utdata, felhantering och sessionssäkerhet.

3.3 Kräva säker implementering av mekanismer för autentisering, auktorisering och åtkomstkontroll i enlighet med organisationens policyer för identitets- och åtkomsthantering.

3.4 Kräva säker interaktion med API:er, webbgränssnitt och tredjepartskomponenter med hjälp av godkända protokoll och säkerhetskontroller.

3.5 Möjliggöra tidig upptäckt och riskreducering av sårbarheter genom statisk och dynamisk analys, kodgranskningar och hotmodellering.

3.6 Skydda känsliga data i enlighet med regulatoriska krav genom att tillämpa kryptering, klassificering och bevarandelogik.

3.7 Säkerställa kontinuerlig validering av applikationers säkerhetsstatus efter driftsättning genom testning, övervakning och revisionsberedskap.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare för denna policy och säkerställer att den är i linje med organisationens informationssäkerhetsstrategi och riskläge.

4.1.2 Godkänner säkerhetskrav för applikationer och säkerställer att obligatoriska kontroller tillämpas inom utveckling och upphandling.

4.2 Applikationssäkerhetsansvarig / DevSecOps-chef

4.2.1 Definierar grundläggande säkerhetskontroller och testmetoder för applikationskomponenter.

4.2.2 Utövar tillsyn över säker integration av verktyg såsom SAST, DAST, IAST och SCA i programvaruleveransprocessen.

4.2.3 Förvaltar checklistan för säkerhetskrav för applikationer och tillhörande valideringskriterier.

[... 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 Offentliggöranden av kritiska sårbarheter som påverkar vanliga ramverk eller beroenden

9.1.2 Uppdateringar av regulatoriska skyldigheter för applikationssäkerhet, till exempel NIS2 och DORA

9.1.3 Större förändringar i organisationens arbetssätt för programvaruutveckling, verktygsstöd eller molnarkitektur

9.1.4 Iakttagelser från internrevision eller externa penetrationstester

9.2 Granskningen ska ledas av applikationssäkerhetsansvarig i samordning med informationssäkerhetschef (CISO), DevOps Engineering, juridik, upphandling och QA-ansvariga.

9.3 Alla revideringar ska versionshanteras i ISMS-registret för dokumentstyrning och distribueras till alla berörda utvecklings- och produktteam.

9.4 Ersatta versioner ska arkiveras i minst tre år för att säkerställa spårbarhet, revisionsbarhet och stöd för utredning av överträdelser.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer grunden för skydd av system och data, där kontroller på applikationsnivå krävs för att förhindra obehörig åtkomst, dataläckage och utnyttjande.

10.2 P4 – Åtkomstkontrollpolicy. Definierar standarder för identitets- och sessionshantering som ska tillämpas av alla applikationer, inklusive stark autentisering, principen om minsta privilegium och krav på åtkomstgranskning.

10.3 P5 – Ändringshanteringspolicy. Reglerar överföring av applikationskod och konfigurationer till produktionsmiljöer och säkerställer att otillåtna eller otestade ändringar blockeras.

10.4 P17 – Policy för dataskydd och integritet. Kräver att applikationer tillämpar dataskydd genom design och säkerställer laglig hantering, kryptering och bevarande av personuppgifter och känsliga data i alla miljöer.

10.5 P24 – Policy för säker utveckling. Tillhandahåller det övergripande ramverket för att integrera säkerhet i SDLC, där denna policy anger de konkreta krav och tekniska kontroller som ska genomföras på applikationsnivå.

10.6 P30 – Policy för incidenthantering. Kräver strukturerad hantering av säkerhetsincidenter inom applikationssäkerhet, inklusive sårbarheter som identifieras efter driftsättning eller vid penetrationstestning, och beskriver eskalering, begränsning och återställning.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:2022

11.1.1 Klausul 8.1 – Operativ planering och styrning: Kräver att applikationssäkerhet integreras i processer och system för att säkerställa konfidentialitet, riktighet och tillgänglighet.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollerna 8.25–8.26: Beskriver förväntningarna på säkerhet på applikationsnivå, inklusive säker kodningspraxis, hotmodellering, arkitekturella kontroller och validering av tredjepartsprogramvara.

11.2.2 Bilaga A kontroll 8.25 – Säker utvecklingslivscykel: Kräver att säkerhet integreras genom hela applikationens livscykel.

11.2.3 Bilaga A kontroll 8.26 – Säkerhetskrav för applikationer: Kräver att tekniska kontroller definieras och tillämpas för att skydda applikationer mot missbruk och kompromettering.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Säkerhetstestning och utvärdering av utvecklare: Kräver statisk testning, dynamisk testning och penetrationstestning under utveckling.

11.3.2 SA-15 – Utvecklingsprocess, standarder och verktyg: Fastställer formella standarder för säker applikationsutveckling.

11.3.3 SI-10 – Validering av informationsindata: Kräver kontrollmekanismer för att förhindra injektionsattacker och attacker mot parsning.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 25 – Dataskydd genom design och som standard: Kräver att dataskydd och integritet integreras i applikationslogik och arbetsflöden.

11.4.2 Artikel 32 – Säkerhet i behandlingen: Kräver lämpliga tekniska åtgärder, såsom indatavalidering, kryptering och säkra åtkomstkontroller.

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

11.5.1 Artikel 21(2)(f): Kräver hantering av sårbarheter och säker praxis genom hela applikationens livscykel för väsentliga och viktiga entiteter.

11.5.2 Artikel 23 – Rapportering av säkerhetsincidenter: Kräver funktioner för loggning och övervakning på applikationsnivå för att upptäcka och rapportera betydande incidenter.

11.6 DORA-förordningen (2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Förpliktar finansiella entiteter att säkerställa att applikationer är säkra, testade och motståndskraftiga mot cyberhot.

11.6.2 Artikel 11 – Testning av IKT-verktyg: Uppmuntrar regelbunden penetrationstestning och red team-övningar för kritiska applikationer och tjänster.

11.7 COBIT 2019

11.7.1 BAI03 – Hantera identifiering och utveckling av lösningar: Fastställer krav på design och kontroller under applikationsutveckling.

11.7.2 BAI09 – Hantera applikationer: Betonar säkert underhåll, övervakning och vidareutveckling av applikationer i drift.

11.7.3 DSS05 – Hantera säkerhetstjänster: Kopplar skydd av applikationer till organisationens bredare säkerhetsoperationer och kontroller.