					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P25S					Dokumenttitel: **Policy för applikationssäkerhetskrav**							
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/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Operativa kontroller, inklusive applikationssäkerhet
ISO/IEC 27002:2022	Kontroller 8.25–8.26	Säker design, utveckling, testning och kodgranskning
NIST SP 800-53 Rev.5	SA-11, SI-10	Utvecklar- och applikationstestning, kodanalys samt förebyggande av brister
EU:s GDPR	Artikel 25	Integritetsskydd genom design och dataskydd som standard
EU:s NIS2-direktiv	Artikel 21(2)(a), (e)	Tekniska åtgärder för att säkra applikationer och upptäcka risker
EU:s DORA-förordning	Artiklar 9(2)(c), 10(2)(c)	Applikationssäkerhet för digital operativ motståndskraft
COBIT 2019	BAI03	Hantering av säker utveckling och anskaffning av programvara

1. Syfte

1.1 Denna policy fastställer de lägsta obligatoriska kontrollerna för applikationssäkerhet som gäller för all programvara och alla systemlösningar som används av organisationen, oavsett om de utvecklas internt eller anskaffas från externa leverantörer.

1.2 Den säkerställer att applikationer utformas, implementeras och underhålls för att skydda kunddata, personuppgifter om anställda och verksamhetsinformation mot obehörig åtkomst, missbruk, ändring eller förstöring.

1.3 Denna policy stödjer organisationens arbete med att uppnå och upprätthålla certifiering enligt ISO/IEC 27001, uppfylla skyldigheter enligt GDPR och NIS2 samt minska operativa risker kopplade till osäkra produktionssättningar av programvara.

1.4 Den bidrar till att etablera ett enhetligt och verifierbart arbetssätt för applikationssäkerhet för SME genom att fastställa en gemensam checklista över säkerhetsfunktioner och arbetsmetoder, anpassad för miljöer med begränsade interna tekniska resurser.

2. Omfattning

2.1 Denna policy gäller för alla applikationer, system, verktyg och plattformar som:

2.1.1 utvecklas internt, anpassas eller skriptas för intern användning

2.1.2 anskaffas som kommersiell programvara, SaaS eller system i molnmiljö

2.1.3 behandlar, lagrar eller överför personuppgifter, verksamhetsdokumentation eller känslig operativ information

2.1.4 används av anställda, entreprenörer, tredjepartsleverantörer, kunder eller partners via interna nätverk, internet eller mobila plattformar

2.2 Policyn omfattar:

2.2.1 utvecklare (interna eller kontrakterade)

2.2.2 programvaruleverantörer och molntjänstleverantörer

2.2.3 IT-supportpersonal eller administratörer med ansvar för driftsättning och support

2.2.4 applikationsägare och verksamhetsanvändare som deltar i godkännande och uppföljning av system

3. Mål

3.1 Att säkerställa att alla applikationer som används av organisationen har inbyggda och verifierbara säkerhetskontroller som minskar vanliga tekniska sårbarheter i programvara.

3.2 Att skydda konfidentialitet, riktighet och tillgänglighet för data som behandlas av applikationer, oavsett var de driftas.

3.3 Att kräva formell testning, granskning och validering av applikationssäkerhet innan en ny applikation eller en större uppdatering godkänns för produktionsanvändning.

3.4 Att möjliggöra konsekvent och säker hantering av autentiseringsuppgifter, sessionsdata och åtkomsträttigheter i alla verksamhetskritiska system.

3.5 Att kräva säker revisionsloggning, spårbarhet och övervakningsfunktioner i alla applikationer för att stödja upptäckt av och hantering av misstänkt aktivitet.

3.6 Att minska rättsliga risker och risker för bristande regelefterlevnad genom att säkerställa att applikationer uppfyller tillämpliga regulatoriska säkerhetskrav.

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Har det övergripande ansvaret för applikationssäkerhet i hela organisationen.

4.1.2 Godkänner denna policy och säkerställer att alla anskaffningar och utvecklingsprojekt följer den.

4.1.3 Säkerställer att leverantörer och tjänsteleverantörer omfattas av avtalsvillkor avseende krav på applikationssäkerhet.

4.1.4 Granskar och godkänner undantag från riskkrav när full efterlevnad inte kan uppnås på grund av verksamhetsmässiga begränsningar.

4.2 Applikationsägare (om sådan har utsetts)

4.2.1 Identifierar applikationsspecifika säkerhetsbehov vid systemval eller projektstart.

4.2.2 Verifierar att centrala funktioner såsom inloggningsskydd, kryptering och aktivitetsloggning ingår.

4.2.3 Deltar i riskgranskningar inför driftsättning och bekräftar att säkerhetskontrollerna uppfyller verksamhetens behov.

[... 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 kalenderår för att:

9.1.1 återspegla förändringar i regulatoriska krav (t.ex. GDPR, NIS2, DORA)

9.1.2 införliva nya eller framväxande hot och angreppstekniker

9.1.3 uppdatera språk och krav så att de återspeglar förändringar i plattformar, leverantörer eller utvecklingsmetoder

9.2 Interimistiska granskningar ska även genomföras när:

9.2.1 nya applikationer införs

9.2.2 befintliga applikationer genomgår väsentliga uppdateringar eller integrationer

9.2.3 en applikationsrelaterad incident eller överträdelse inträffar

9.2.4 nya risker identifieras genom externa hotunderrättelser eller branschvarningar

9.3 Alla uppdateringar av denna policy ska:

9.3.1 godkännas av verkställande direktör

9.3.2 dokumenteras med versionshistorik och skäl till ändringen

9.3.3 kommuniceras till alla anställda, utvecklare och leverantörer som deltar i hantering av applikationer

9.3.4 lagras på ett säkert sätt för revision och regelefterlevnad

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds direkt av och bidrar till tillämpningen av följande SME-anpassade säkerhetspolicyer:

10.1.1 P2S – Policy för styrningsroller och ansvar: Tilldelar ansvar för att godkänna applikationer, tillämpa policyn och hantera leverantörer.

10.1.2 P4S – Policy för åtkomstkontroll: Säkerställer att applikationsåtkomst är i linje med principen om minsta privilegium och principer för sessionskontroll.

10.1.3 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att användare och utvecklare får utbildning i att identifiera och rapportera applikationsrelaterade hot.

10.1.4 P17S – Policy för dataskydd och integritet: Tillhandahåller dataskyddsåtgärder som ska tillämpas av alla applikationer som behandlar personuppgifter.

10.1.5 P14S – Policy för databevarande och bortskaffande: Reglerar hur loggar, säkerhetskopior och känsliga uppgifter som genereras av applikationer ska bevaras, arkiveras och förstöras på ett säkert sätt.

10.1.6 P30S – Policy för incidenthantering: Beskriver åtgärder för att identifiera, rapportera och begränsa applikationsrelaterade säkerhetshändelser.

10.2 Tillsammans säkerställer dessa policyer att applikationssäkerhet är fullt integrerad i organisationens ledningssystem för informationssäkerhet och att förmågan att visa efterlevnad kan upprätthållas vid revision.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver att organisationer fastställer operativa kontroller för att hantera informationssäkerhetsrisker, inklusive sådana som rör applikationer och programvarusystem.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – Anger att säker design, utveckling och kodgranskning ska genomföras för alla applikationer, inklusive sådana som tillhandahålls av leverantörer.

11.2.2 Kontroll 8.26 – Rekommenderar formell testning av säkerhetskontroller i applikationer, särskilt inom områden som åtkomstkontroll, indatavalidering och sessionshantering.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Anger krav för utvecklartestning, kodanalys och dynamisk skanning av applikationer före driftsättning.

11.3.2 SI-10 – Behandlar upptäckt och förebyggande av vanliga programvarubrister, med betoning på utvecklares medvetenhet och tekniska skyddsåtgärder.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 25 – ”integritetsskydd genom design och dataskydd som standard” kräver att integritet och säkerhet byggs in i applikationers grundläggande utformning när de hanterar personuppgifter.

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

11.5.1 Artikel 21(2)(a) och (e) – Kräver att väsentliga och viktiga entiteter genomför tekniska åtgärder för att säkra applikationer och upptäcka programvarurelaterade risker.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9(2)(c), 10(2)(c) – Kräver att SME inom finanssektorn bygger in säkerhetskontroller på applikationsnivå och genomför regelbundna bedömningar för att upprätthålla digital operativ motståndskraft.

11.7 COBIT 2019

11.7.1 BAI03 – ”Manage Solutions Identification and Build” vägleder utveckling eller anskaffning av säker programvara i linje med risk, regelefterlevnad och verksamhetskrav, även i SME-miljöer med begränsade resurser.