					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P25S					Dokumenttitel: **Politik for krav til applikationssikkerhed**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	operationelle kontroller, herunder applikationssikkerhed
ISO/IEC 27002:2022	Kontroller 8.25–8.26	sikkert design, udvikling, test og kodegennemgang
NIST SP 800-53 Rev.5	SA-11, SI-10	udviklertest/applikationstest, kodeanalyse, forebyggelse af fejl
EU GDPR	Artikel 25	databeskyttelse gennem design og standardindstillinger
EU NIS2	Artikel 21(2)(a), (e)	tekniske foranstaltninger til sikring af applikationer og identifikation af risici
EU DORA	Artikel 9(2)(c), 10(2)(c)	applikationssikkerhed som led i digital operationel robusthed
COBIT 2019	BAI03	styring af sikker udvikling og anskaffelse af software

1. Formål

1.1 Denne politik fastsætter de minimumskrav til applikationssikkerhed, der gælder for alle software- og systemløsninger, som anvendes af organisationen, uanset om de er udviklet internt eller anskaffet fra eksterne leverandører.

1.2 Den sikrer, at applikationer designes, implementeres og vedligeholdes, så kunde-, medarbejder- og forretningsdata beskyttes mod uautoriseret adgang, misbrug, ændring eller destruktion.

1.3 Denne politik understøtter organisationens arbejde med at opnå og opretholde ISO/IEC 27001-certificering, opfylde forpligtelser efter GDPR og NIS2 samt reducere driftsmæssige risici forbundet med usikre softwareimplementeringer.

1.4 Den bidrager til en ensartet og revisionsklar tilgang til applikationssikkerhed for SMV'er ved at fastlægge en fælles tjekliste over sikkerhedsfunktioner og praksisser, tilpasset miljøer med begrænsede interne tekniske ressourcer.

2. Omfang

2.1 Denne politik gælder for alle applikationer, systemer, værktøjer og platforme, som:

2.1.1 er udviklet internt, tilpasset eller scriptet til intern brug

2.1.2 er anskaffet som kommerciel software, SaaS eller cloudbaserede systemer

2.1.3 behandler, opbevarer eller overfører personoplysninger, forretningsoptegnelser eller følsomme driftsoplysninger

2.1.4 tilgås af medarbejdere, kontrahenter, kunder eller partnere via interne netværk, internettet eller mobile platforme

2.2 Politikken omfatter:

2.2.1 udviklere (interne eller kontraherede)

2.2.2 softwareleverandører og udbydere af cloudtjenester

2.2.3 IT-supportpersonale eller administratorer med ansvar for idriftsættelse og support

2.2.4 applikationsansvarlige og forretningsbrugere, der indgår i godkendelse og tilsyn med systemer

3. Mål

3.1 At sikre, at alle applikationer, som organisationen anvender, har indbyggede og verificerbare sikkerhedskontroller, der reducerer almindelige softwaresårbarheder.

3.2 At beskytte fortrolighed, integritet og tilgængelighed for data, der behandles af applikationer, uanset hvor de hostes.

3.3 At kræve formel test, gennemgang og validering af applikationssikkerhed, før en ny applikation eller en væsentlig opdatering godkendes til brug i produktionsmiljøet.

3.4 At sikre ensartet og sikker håndtering af brugerlegitimationsoplysninger, sessionsdata og adgangsrettigheder på tværs af alle forretningskritiske systemer.

3.5 At kræve sikker logning, revisionsspor og overvågningsfunktioner i alle applikationer for at understøtte identifikation og håndtering af mistænkelig aktivitet.

3.6 At reducere juridiske risici og compliance-risici ved at sikre, at applikationer opfylder gældende regulatoriske sikkerhedskrav.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for applikationssikkerhed på tværs af organisationen.

4.1.2 Godkender denne politik og sikrer, at alle anskaffelser eller udviklingsprojekter efterlever den.

4.1.3 Sikrer, at leverandører og tjenesteudbydere kontraktligt forpligtes til at opfylde kravene til applikationssikkerhed.

4.1.4 Gennemgår og godkender risikoundtagelser, hvor fuld efterlevelse ikke kan opnås på grund af forretningsmæssige begrænsninger.

4.2 Applikationsansvarlig (hvis udpeget)

4.2.1 Identificerer applikationsspecifikke sikkerhedsbehov ved systemvalg eller projektopstart.

4.2.2 Verificerer, at centrale funktioner som loginbeskyttelse, kryptering og aktivitetslogning indgår.

4.2.3 Deltager i gennemgange forud for idriftsættelse og bekræfter, at sikkerhedskontroller opfylder forretningens behov.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås af direktør mindst én gang pr. kalenderår for at:

9.1.1 afspejle ændringer i regulatoriske krav (f.eks. GDPR, NIS2, DORA)

9.1.2 indarbejde nye eller fremvoksende trusler og angrebsteknikker

9.1.3 opdatere formuleringer og krav, så de afspejler ændringer i platforme, leverandører eller udviklingsmetoder

9.2 Der skal også gennemføres ekstraordinære gennemgange, når:

9.2.1 nye applikationer indføres

9.2.2 eksisterende applikationer gennemgår væsentlige opdateringer eller integrationer

9.2.3 der opstår en applikationsrelateret hændelse eller et brud

9.2.4 nye risici identificeres på baggrund af eksterne meddelelser eller branchevarsler

9.3 Alle opdateringer til denne politik skal:

9.3.1 godkendes af direktør

9.3.2 dokumenteres med versionshistorik og begrundelse for ændringen

9.3.3 kommunikeres til alle medarbejdere, udviklere og leverandører, der indgår i applikationsstyringen

9.3.4 opbevares sikkert som reference for revision og efterlevelse

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes direkte af og bidrager til håndhævelsen af følgende SME-tilpassede sikkerhedspolitikker:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Tildeler ansvar for godkendelse af applikationer, håndhævelse af politikken og leverandørstyring.

10.1.2 P4S – Politik for adgangskontrol: Sikrer, at adgang til applikationer er i overensstemmelse med princippet om mindst privilegium og sessionsstyring.

10.1.3 P8S – Politik for bevidsthed om informationssikkerhed og uddannelse: Sikrer, at brugere og udviklere er uddannet i at genkende og rapportere applikationsrelaterede trusler.

10.1.4 P17S – Databeskyttelses- og privatlivspolitik: Fastlægger databeskyttelsesforanstaltninger, som skal håndhæves af enhver applikation, der behandler personoplysninger.

10.1.5 P14S – Dataopbevarings- og bortskaffelsespolitik: Styrer, hvordan logfiler, sikkerhedskopier og følsomme data genereret af applikationer skal opbevares, arkiveres og destrueres sikkert.

10.1.6 P30S – Politik for hændelseshåndtering: Beskriver de trin, der skal følges for at identificere, rapportere og inddæmme applikationsrelaterede sikkerhedshændelser.

10.2 Samlet set sikrer disse politikker, at applikationssikkerhed er fuldt integreret i organisationens ledelsessystem for informationssikkerhed (ISMS) og er revisionsklar.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kræver, at organisationer etablerer operationelle kontroller til håndtering af informationssikkerhedsrisici, herunder risici relateret til applikationer og softwaresystemer.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.25 – Anbefaler implementering af praksis for sikkert design, udvikling og kodegennemgang på tværs af alle applikationer, herunder dem, der leveres af leverandører.

11.2.2 Kontrol 8.26 – Anbefaler formel test af sikkerhedskontroller i applikationer, særligt inden for adgangsstyring, inputvalidering og sessionsstyring.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Specificerer krav til udviklertest, kodeanalyse og dynamisk scanning af applikationer før idriftsættelse.

11.3.2 SI-10 – Omhandler identifikation og forebyggelse af almindelige softwarefejl med vægt på udviklerbevidsthed og tekniske sikkerhedsforanstaltninger.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 25 – „databeskyttelse gennem design og standardindstillinger“ kræver, at databeskyttelse og sikkerhed indbygges i det grundlæggende design af applikationer, der behandler personoplysninger.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(a) og (e) – Kræver, at væsentlige og vigtige enheder implementerer tekniske foranstaltninger til at sikre applikationer og identificere risici relateret til software.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9(2)(c), 10(2)(c) – Kræver, at SMV'er i den finansielle sektor indbygger sikkerhedskontroller på applikationsniveau og gennemfører regelmæssige vurderinger for at opretholde digital operationel robusthed.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build“ giver vejledning om udvikling eller anskaffelse af sikker software i overensstemmelse med risici, compliance og forretningskrav – også i ressourcebegrænsede SMV-miljøer.