					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P24S					Dokumenttitel: **Politik for sikker udvikling**							
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	Clause 8	Relevante sikkerhedskontroller for operationelle praksisser, herunder sikker udvikling
ISO/IEC 27002:2022	Controls 8.25–8.27	Omfatter sikker softwareudviklingslivscyklus, test og sikkerhedsansvar for tredjepartsudviklere
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Omhandler sikker SDLC, adgangsstyring og håndtering af sårbarheder under udvikling
EU GDPR	Article 25	Kræver databeskyttelse gennem design og standardindstillinger i softwareudvikling
EU NIS2	Article 21(2)(a), (e), (h)	Pålægger politikker for sikker udvikling, kontrol med brug af open source og dokumentation for risikobegrænsende foranstaltninger
EU DORA	Articles 6(7), 9(1)(c), 10(2)(c)	Livscyklussikkerhed for kritiske IKT-systemer i den finansielle sektor
COBIT 2019	BAI	Rammeværk for struktureret, sporbar og robust styring af sikker udvikling

1. Formål

1.1 Denne politik skal sikre, at al software, alle scripts og alle webbaserede værktøjer, som organisationen eller dens eksterne parter udvikler eller ændrer, udvikles sikkert, så risikoen for sårbarheder, uautoriseret adgang til data eller driftsafbrydelser minimeres.

1.2 Den fastsætter obligatoriske krav til sikker udvikling og sikker kodningspraksis, som alle interne udviklere, kontrahenter og leverandører skal følge, uanset projektets størrelse eller kompleksitet.

1.3 Denne politik skal beskytte kundedata, forebygge brud og sikre, at software, som udvikles eller tilpasses af eller for organisationen, kan bestå sikkerhedsrevisioner, opfylde lovkrav (f.eks. GDPR, NIS2 og DORA) og understøtte certificering efter ISO/IEC 27001.

2. Omfang

2.1 Denne politik gælder for alle personer og enheder, der på organisationens vegne udvikler, tilpasser, idriftsætter eller administrerer følgende:

2.1.1 Websites, applikationer eller automatiseringsværktøjer

2.1.2 Internt udviklede scripts eller software

2.1.3 Kode udviklet af tredjepartsudviklere eller freelancere

2.1.4 Plugins, biblioteker og softwarekomponenter, der integreres i produktionssystemer

2.2 Den omfatter alle miljøer, der anvendes til udviklingsaktiviteter, herunder:

2.2.1 Udviklings- og testmiljøer

2.2.2 Staging- og præproduktionsmiljøer

2.2.3 Produktionssystemer, der anvendes til at afvikle kode udviklet specifikt til organisationen

2.3 Politikken regulerer også håndtering af data under udvikling og idriftsættelse, særligt enhver anvendelse af produktionsdata i ikke-produktionsmiljøer.

3. Mål

3.1 At forhindre introduktion af sikkerhedsfejl eller sårbarheder i software, der er specialudviklet eller udviklet af tredjeparter.

3.2 At sikre, at sikker kodningspraksis og forebyggelse af sårbarheder indarbejdes i alle faser af softwareudviklingslivscyklussen.

3.3 At reducere risici forbundet med brug af open source-komponenter eller tredjepartskomponenter ved at kræve korrekt vurdering og sporing.

3.4 At kræve formel kodegennemgang og applikationssikkerhedstest før frigivelse.

3.5 At styre adgang til udviklingsmiljøer og sikre adskillelse fra produktionssystemer i drift.

3.6 At opfylde obligatoriske krav efter internationale standarder og regler (f.eks. ISO/IEC 27001, GDPR, DORA og NIS2).

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender og ejer denne politik.

4.1.2 Sikrer, at al softwareudvikling, både intern og udliciteret, efterlever denne politik.

4.1.3 Gennemgår og underskriver udviklings- eller serviceaftaler, der indeholder klausuler om sikker udvikling.

4.1.4 Verificerer leverandørers efterlevelse gennem regelmæssige opfølgninger eller ved at anmode om sikkerhedsdokumentation.

4.2 Intern udvikler eller applikationsejer

4.2.1 Følger sikker kodningspraksis og sikre udrulningsprocedurer.

4.2.2 Anvender tjeklisten for sikker udvikling i hvert projekt.

4.2.3 Validerer sikkerheden i alle open source-komponenter eller tredjepartskomponenter, der anvendes.

4.2.4 Rapporterer straks alle identificerede sårbarheder til direktøren.

[... 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 direktøren mindst én gang årligt for at:

9.1.1 Verificere fortsat overholdelse af ISO/IEC 27001, GDPR, NIS2 og DORA

9.1.2 Afspejle opdaterede trusler eller ændringer i bedste praksis for sikker udvikling

9.1.3 Sikre kompatibilitet med nye værktøjer, platforme eller leverandørforhold

9.2 Mellemliggende gennemgange skal udløses af:

9.2.1 Enhver rapporteret softwarerelateret sikkerhedshændelse

9.2.2 Indførelse af et nyt udviklingsframework eller en ny hostingplatform

9.2.3 En ændring i tredjepartsudviklingspartnere

9.2.4 Opdateringer i regulering, der påvirker software eller sikkerhedsforpligtelser

9.3 Alle ændringer i denne politik skal:

9.3.1 Dokumenteres med dato, resumé af ændringen og godkendelse fra direktøren

9.3.2 Kommunikeres klart til alt internt og eksternt udviklingspersonale

9.3.3 Opbevares som en del af organisationens versionsstyring og ændringshistorik for politikker

9.4 Opdaterede versioner skal være let tilgængelige, enten via interne platforme, trykt dokumentation eller cloudtjenester, som leverandører har adgang til.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter og afhænger af en effektiv implementering af flere andre SME-politikker:

10.1.1 P2S - Politik for styringsroller og ansvarsområder: Etablerer ansvarlighed for tildeling og verifikation af sikkerhedskontroller for udvikling på tværs af projekter og leverandører.

10.1.2 P4S - Politik for adgangskontrol: Fastlægger grundlæggende regler for at begrænse adgang til udviklingsmiljøer og koderepositorier, herunder funktionsadskillelse.

10.1.3 P8S - Politik for awareness om informationssikkerhed og uddannelse: Sikrer, at interne udviklere og kontrahenter forstår sikker kodningspraksis og tilhørende sikkerhedsansvar.

10.1.4 P17S - Databeskyttelses- og privatlivspolitik: Præciserer, hvordan personoplysninger skal håndteres under udvikling, test og logningsprocesser for at sikre overholdelse af GDPR.

10.1.5 P30S - Politik for hændelseshåndtering: Definerer, hvordan udviklingsrelaterede sikkerhedshændelser skal rapporteres, vurderes og afhjælpes, herunder koderelaterede eksponeringer.

10.2 Disse politikker virker samlet for at sikre, at sikker udvikling kan gennemføres og dokumenteres, også i en lille eller ikke-teknisk organisation.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Clause 8 - Kræver implementering af operationelle kontroller, herunder sikker udvikling, som er tilpasset forretningsmål og risikobillede.

11.2 ISO/IEC 27002

11.2.1 Control 8.25 - Anbefaler, at sikkerhed integreres gennem hele softwarelivscyklussen, herunder kildekodestyring, versionsstyring og udvikleradgang.

11.2.2 Control 8.26 - Specificerer metoder til applikationstest og verifikation af sikkerhedsfunktionalitet før idriftsættelse.

11.2.3 Control 8.27 - Kræver, at tredjepartsudviklere efterlever de samme udviklingsstandarder, og at deres sikkerhedsansvar er klart defineret.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 til SA-15 - Definerer processer for sikker udvikling, herunder adgangsstyring for udviklere, test, trusselsmodellering og dokumentation.

11.3.2 SI-10 - Kræver, at udviklere identificerer og afbøder almindelige svagheder i software og anvender automatiserede værktøjer, hvor det er relevant.

11.4 EU GDPR (2016/679)

11.4.1 Article 25 - "Databeskyttelse gennem design og standardindstillinger" kræver, at sikkerheds- og databeskyttelsesforanstaltninger integreres under design og udvikling af software, særligt hvor der behandles personoplysninger.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Article 21(2)(a), (e) og (h) - Kræver politikker for sikker udvikling, kontrol med brug af open source og dokumenteret risikoafbødning for applikationsrelaterede risici i væsentlige og vigtige enheder.

11.6 EU DORA (2022/2554)

11.6.1 Articles 6(7), 9(1)(c) og 10(2)(c) - Pålægger sikkerhedsforpligtelser i udviklingslivscyklussen for enheder i den finansielle sektor, herunder SMV'er, særligt for kritiske IKT-systemer.

11.7 COBIT 2019

11.7.1 BAI03 - "Manage Solutions Identification and Build" understøtter implementering af strukturerede udviklingskontroller med fokus på sikkerhed, sporbarhed og robusthed, tilpasset begrænsninger i SMV'er.