					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P24					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**

1. Formål

1.1 Denne politik fastsætter obligatoriske sikkerhedskrav for aktiviteter vedrørende software- og systemudvikling i organisationen, herunder interne projekter, outsourced udvikling og integration af kode fra tredjeparter.

1.2 Formålet er at sikre, at sikkerhed er indarbejdet gennem hele systemudviklingslivscyklussen (SDLC), og at sårbarheder identificeres, afbødes og forebygges inden idriftsættelse i produktionsmiljøet.

1.3 Denne politik understøtter efterlevelsen af ISO/IEC 27001:2022 klausul 8.1 og Anneks A-kontrollerne 8.25–8 ved at standardisere styringen af sikker udvikling, praksis for kodevalidering og tilsyn med udvikling udført af tredjeparter.

2. Omfang

2.1 Denne politik gælder for alle:

2.1.1 Internt eller eksternt udviklede softwareløsninger, applikationer, scripts, integrationer og automatiseringsværktøjer

2.1.2 Udviklingsteams, produktejere, DevOps-teams, QA, arkitekter, projektledere og kontraktansatte

2.1.3 SDLC-miljøer, herunder udviklings-, test-, staging- og præproduktionssystemer

2.1.4 Open source-komponenter og tredjepartskomponenter, der integreres i interne applikationer

2.1.5 Software, der er implementeret i on-premises-infrastruktur, private cloudmiljøer, hybride miljøer eller offentlige cloudmiljøer

2.2 Alle brugere og enheder, der deltager i systemudvikling, test eller implementering inden for organisationens kontekst, er omfattet af denne politik, herunder managed service providers (MSP'er) og platformsleverandører.

3. Mål

3.1 Indarbejde sikkerhedskontroller i alle faser af softwareudvikling, fra design til implementering, så risikoreduktion er proaktiv og løbende.

3.2 Forebygge introduktion af udnyttelige sårbarheder såsom injektionsfejl, usikker autentifikation og eksponering for kendte svagheder i tredjepartskomponenter.

3.3 Etablere og håndhæve praksis for sikker kodning tilpasset OWASP, SANS CWE og frameworkspecifikke retningslinjer.

3.4 Sikre, at al kode gennemgår peer review, automatiseret analyse og sikkerhedsvalidering før implementering.

3.5 Styre udviklingsrisici, der udspringer af outsourced aktiviteter, inkludering af kode fra tredjeparter og genbrug af open source-software.

3.6 Beskytte udviklings-, test- og stagingmiljøer mod uautoriseret adgang og forhindre brug af produktionsdata uden godkendt datamaskering eller anonymisering.

3.7 Fremme sikkerhedsbevidsthed blandt udviklere, produktledere og kvalitetssikringsmedarbejdere gennem rollebaserede træningsmoduler og løbende opdateringer om nye risici.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer, at krav til sikker udvikling håndhæves i hele organisationen.

4.1.2 Godkender standarder for sikker kodning og udviklingsaftaler med tredjeparter.

4.1.3 Validerer beslutninger om risikobehandling for uløste eller udskudte sårbarheder.

4.2 Ansvarlig for applikationssikkerhed / DevSecOps-ansvarlig

4.2.1 Udarbejder, vedligeholder og forankrer retningslinjer for sikker kodning.

4.2.2 Integrerer statisk og dynamisk sikkerhedstest i CI/CD-pipelines.

4.2.3 Gennemfører sikkerhedsgennemgang af kode og fastsætter obligatoriske afhjælpende handlinger.

[... 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 årligt eller oftere som reaktion på:

9.1.1 Større ændringer i udviklingsmetoder eller DevOps-værktøjer

9.1.2 Væsentlige sikkerhedshændelser, der udspringer af applikationssårbarheder

9.1.3 Ændringer i regulatoriske krav vedrørende sikker software (f.eks. GDPR, DORA)

9.1.4 Nye branchestandarder eller ny trusselsinformation (f.eks. OWASP Top 10, SLSA, MITRE CWE)

9.2 Gennemgang af politikken skal ledes af den ansvarlige for applikationssikkerhed i koordinering med CISO, softwarearkitekter, QA-ledelse og juridisk rådgivning (for forhold vedrørende kode fra tredjeparter).

9.3 Alle revisioner skal registreres i ISMS-dokumentstyringsregisteret, være versionsstyrede og kommunikeres til berørte teams via release notes eller obligatorisk træning.

9.4 Ældre versioner skal opbevares i arkivrepositoriet af hensyn til juridisk holdbarhed og revisionsspor.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger det strategiske mandat for at indarbejde sikkerhed i alle informationssystemer, hvor sikker udvikling er en grundlæggende operationel kontrol.

10.2 P4 – Politik for adgangskontrol. Definerer kontrolforanstaltninger til begrænsning af adgang til udviklingsmiljøer, repositorier, build-værktøjer og CI/CD-pipelines.

10.3 P5 – Politik for ændringsstyring. Sikrer, at kodeændringer, releases og implementeringer er underlagt korrekt godkendelse, planlægning af tilbagerulning og verifikation efter implementering.

10.4 P12 – Politik for styring af aktiver. Understøtter registrering af udviklingsmiljøer, kilderepositorier og build-systemer som styrede aktiver underlagt klassificering og beskyttelse.

10.5 P22 – Politik for logning og overvågning. Gælder for udviklingspipelines og sikrer, at build-processer, kodepromoveringer og implementeringshændelser logges, overvåges og analyseres for sikkerhedsanomalier.

10.6 P30 – Politik for hændelseshåndtering. Fastlægger rammen for analyse og håndtering af sikkerhedsfejl, der opdages efter implementering eller under sikkerhedstest af applikationer.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – operationel planlægning og styring: Kræver integration af processer og kontroller for sikker udvikling i driften.

11.2 ISO/IEC 27002:2022 – Kontroller 8.25–8

11.2.1 Anneks A-kontrol 8.25 – Livscyklus for sikker udvikling: Kræver formel indarbejdelse af sikkerhed i softwaredesign og -udvikling.

11.2.2 Anneks A-kontrol 8.26 – Sikkerhedskrav til applikationer: Kræver definition af sikker kodning og sikkerhedsrelaterede acceptkriterier.

11.2.3 Anneks A-kontrol 8.27 – Sikker systemarkitektur og engineering-principper: Kræver anvendelse af principper for sikkerhedsdesign og afbødning af kendte svagheder.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 til SA-15: Etablerer struktureret praksis for udvikling af applikationssikkerhed, herunder krav til design, kodeintegritet og test.

11.3.2 SI-10 – Validering af informationsinput: Omhandler forsvarsmekanismer til sikker kodning.

11.3.3 SR-3 – Beskyttelse af forsyningskæden: Kræver vurdering af tredjepartssoftware, komponenter og udviklingsleverandører.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 25 – databeskyttelse gennem design og standardindstillinger: Kræver, at sikkerhed og databeskyttelse indarbejdes i systemudvikling.

11.4.2 Artikel 32 – behandlingssikkerhed: Understøtter tekniske foranstaltninger som inputvalidering, adgangskontroller og sikker implementering.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(e–f): Kræver softwareudviklingspraksis, der omfatter sårbarhedsstyring, kodesikkerhed og rapportering af hændelser.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – styring af IKT-risiko: Kræver praksis for sikker udvikling for finansielle enheder, herunder kontroller for softwarekvalitet og afhjælpning af fejl.

11.6.2 Artikel 10 – forretningskontinuitet og test: Tilskynder til grundig test og validering af IKT-systemer, herunder applikationer.

11.7 COBIT 2019

11.7.1 BAI03 – Styring af identifikation og opbygning af løsninger: Regulerer design, udvikling og integration af sikkerhed i nye løsninger.

11.7.2 BAI07 – Styring af ændringsaccept og overgang: Sikrer sikker implementering og evaluering efter implementering.

11.7.3 DSS05 – Styring af sikkerhedstjenester: Anvender sikkerhedsvalidering på softwareleverancer og tjenesteleverance.