					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P25					Dokumenttitel: **Politik for applikationssikkerhedskrav**							
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	Kapitel 8	—
ISO/IEC 27002:2022	Kontroller 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EU GDPR	Artikel 25, 32	—
EU NIS2	Artikel 21(2)(f), 23	—
EU DORA	Artikel 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Formål

1.1 Denne politik fastsætter obligatoriske sikkerhedskrav på applikationslaget for software, der udvikles, anskaffes, integreres eller idriftsættes af organisationen. Den sikrer, at alle applikationer designes, implementeres og vedligeholdes i overensstemmelse med principperne for sikker udvikling, regulatoriske forpligtelser og organisationens risikovillighed.

1.2 Politikken kræver, at sikkerhed indarbejdes gennem hele applikationens livscyklus og omfatter brugergodkendelse, datahåndtering, beskyttelse af grænseflader samt sikker interaktion med API'er og tjenester.

1.3 Ved at anvende denne politik har organisationen til formål at forebygge introduktion af softwaresårbarheder, beskytte følsomme data samt sikre sporbarhed og robusthed mod udnyttelse og misbrug.

2. Omfang

2.1 Denne politik gælder for alle:

2.1.1 Internt udviklede eller eksternt anskaffede applikationer, herunder SaaS-løsninger og specialudviklede værktøjer

2.1.2 Applikationer, der understøtter kritiske forretningsoperationer, kundeadgang eller behandling af regulerede data

2.1.3 Udviklings-, DevOps-, QA-, produkt- og sikkerhedsteams

2.1.4 Tredjepartsudviklere, softwareleverandører og integrationspartnere med adgang til organisationens applikationer eller API'er

2.2 Politikken gælder på tværs af alle miljøer: udvikling, test, staging, produktion og katastrofeberedskab, uanset om de hostes i on-premises-infrastruktur, i private datacentre eller i offentlige cloudmiljøer.

3. Mål

3.1 Fastlægge grundlæggende funktionelle og ikke-funktionelle sikkerhedskrav, som alle applikationer skal opfylde, uanset udviklingsmetode eller teknologistak.

3.2 Sikre integration af beskyttelse på applikationslaget, herunder inputvalidering, outputkodning, fejlhåndtering og sessionssikkerhed.

3.3 Kræve sikker implementering af mekanismer til autentificering, autorisation og adgangsstyring i overensstemmelse med organisationens politikker for identitets- og adgangsstyring.

3.4 Kræve sikker interaktion med API'er, webgrænseflader og tredjepartskomponenter ved anvendelse af godkendte protokoller og sikkerhedskontroller.

3.5 Muliggøre tidlig identifikation og afhjælpning af sårbarheder gennem statisk og dynamisk analyse, kodegennemgang og trusselsmodellering.

3.6 Beskytte følsomme data i overensstemmelse med regulatoriske krav ved at håndhæve kryptering, klassificering og logik for dataopbevaring.

3.7 Sikre løbende validering af applikationers sikkerhedstilstand efter idriftsættelse gennem test, overvågning og revisionsberedskab.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer, at den er tilpasset organisationens informationssikkerhedsstrategi og risikobillede.

4.1.2 Godkender krav til applikationssikkerhed og håndhæver obligatoriske kontroller på tværs af udviklings- og indkøbsfunktioner.

4.2 Applikationssikkerhedsansvarlig / DevSecOps-ansvarlig

4.2.1 Definerer grundlæggende sikkerhedskontroller og testmetoder for applikationskomponenter.

4.2.2 Fører tilsyn med sikker integration af værktøjer som SAST, DAST, IAST og SCA i softwareleveringspipelines.

4.2.3 Vedligeholder tjekliste for krav til applikationssikkerhed og valideringskriterier.

[... 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 hyppigere som følge af:

9.1.1 Oplysninger om kritiske sårbarheder, der påvirker almindelige frameworks eller afhængigheder

9.1.2 Opdateringer af regulatoriske forpligtelser vedrørende applikationssikkerhed (f.eks. NIS2 og DORA)

9.1.3 Større ændringer i organisationens praksis for softwareudvikling, værktøjer eller cloudarkitektur

9.1.4 Konstateringer fra intern revision eller eksterne penetrationstest

9.2 Gennemgangen skal ledes af den applikationssikkerhedsansvarlige i koordinering med CISO, DevOps Engineering, Jura, Indkøb og QA-ledere.

9.3 Alle revisioner skal være versionsstyret i ISMS' dokumentregister og distribueres til alle berørte udviklings- og produktteams.

9.4 Erstattede versioner skal arkiveres i mindst tre år af hensyn til sporbarhed, revisionsparathed og understøttelse af undersøgelser af brud.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger grundlaget for beskyttelse af systemer og data, hvorunder kontroller på applikationsniveau er påkrævet for at forhindre uautoriseret adgang, datalækage og udnyttelse.

10.2 P4 – Politik for adgangskontrol. Definerer standarder for identitets- og sessionsstyring, som alle applikationer skal håndhæve, herunder stærk autentificering, mindst privilegieprincip og krav til gennemgang af adgangsrettigheder.

10.3 P5 – Politik for ændringsstyring. Regulerer overførsel af applikationskode og konfigurationer til produktionsmiljøer og sikrer, at uautoriserede eller ikke-testede ændringer blokeres.

10.4 P17 – Databeskyttelses- og privatlivspolitik. Kræver, at applikationer implementerer databeskyttelse gennem design og standardindstillinger samt sikrer lovlig behandling, kryptering og opbevaring af personoplysninger og følsomme data på tværs af alle miljøer.

10.5 P24 – Politik for sikker udvikling. Angiver den overordnede ramme for at indarbejde sikkerhed i SDLC, mens denne politik fastsætter de konkrete krav og tekniske kontroller, der skal implementeres på applikationslaget.

10.6 P30 – Politik for hændelseshåndtering. Kræver struktureret håndtering af sikkerhedshændelser relateret til applikationer, herunder sårbarheder identificeret efter idriftsættelse eller under penetrationstest, og beskriver procedurer for eskalering, inddæmning og genopretning.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:2022

11.1.1 Kapitel 8.1 – operationel planlægning og styring: Kræver, at applikationssikkerhed indarbejdes i processer og systemer for at sikre fortrolighed, integritet og tilgængelighed.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroller 8.25–8.26: Beskriver forventningerne til sikkerhed på applikationslaget, herunder praksis for sikker kodning, trusselsmodellering, arkitekturkontroller og validering af tredjepartssoftware.

11.2.2 Bilag A, kontrol 8.25 – Secure Development Life Cycle: Kræver integration af sikkerhed gennem hele applikationens livscyklus.

11.2.3 Bilag A, kontrol 8.26 – Application Security Requirements: Kræver definition og håndhævelse af tekniske kontroller, der beskytter applikationer mod misbrug og kompromittering.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Developer Security Testing and Evaluation: Kræver statisk analyse, dynamisk analyse og penetrationstest under udvikling.

11.3.2 SA-15 – Development Process, Standards, and Tools: Fastlægger formelle standarder for sikker applikationsudvikling.

11.3.3 SI-10 – Information Input Validation: Kræver kontrolmekanismer til forebyggelse af injektions- og parsingangreb.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 25 – Data Protection by Design and by Default: Kræver integration af databeskyttelse og privatliv i applikationslogik og arbejdsgange.

11.4.2 Artikel 32 – Security of Processing: Kræver passende tekniske foranstaltninger såsom inputvalidering, kryptering og sikre adgangskontroller.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(f): Kræver håndtering af sårbarheder og praksisser for sikker applikationslivscyklus for væsentlige og vigtige enheder.

11.5.2 Artikel 23 – Reporting of Security Incidents: Nødvendiggør lognings- og overvågningskapaciteter på applikationslaget til at detektere og rapportere væsentlige hændelser.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – ICT Risk Management: Forpligter finansielle enheder til at sikre, at applikationer er sikre, testede og robuste over for cybertrusler.

11.6.2 Artikel 11 – Testing of ICT Tools: Tilskynder til periodisk penetrationstest og red team-øvelser for kritiske applikationer og tjenester.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Fastlægger krav til design og kontroller under applikationsudvikling.

11.7.2 BAI09 – Manage Applications: Fremhæver sikker vedligeholdelse, overvågning og videreudvikling af applikationer i drift.

11.7.3 DSS05 – Manage Security Services: Knytter applikationsbeskyttelse til organisationens bredere sikkerhedsdrift og kontroller.