					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P28					Dokumenttitel: **Politik for outsourcet 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	Klausul 8.1	N/A
ISO/IEC 27002:2022	Kontroller 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
EU GDPR	Artikel 28, 32	N/A
EU NIS2	Artikel 21(2)(a), (h), 23	N/A
EU DORA	Artikel 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Formål

1.1 Denne politik fastsætter obligatoriske kontroller for outsourcing af software- eller systemudvikling til eksterne leverandører, konsulenter eller bureauer og sikrer, at sikre praksisser er indlejret i hele udviklingslivscyklussen.

1.2 Formålet er at forebygge sikkerhedssårbarheder, datatab, eksponering af immaterielle rettigheder (IP) og brud på efterlevelse som følge af eksterne udviklingsengagementer.

1.3 Politikken håndhæver leverandørstyring, praksis for sikker kodning, adgangsstyring, overvågningsforpligtelser og offboarding ved kontraktophør for at opretholde fortrolighed, integritet og tilgængelighed.

2. Omfang

2.1 Denne politik gælder for alle organisatoriske enheder, der engagerer eksterne parter til software- eller systemudvikling, herunder:

2.1.1 Webapplikationer, mobilapplikationer, indlejrede systemer, API'er, scripts, automatiserede arbejdsgange eller platformmoduler

2.1.2 Specialudvikling til interne platforme, kundevendte systemer eller kommercielle produkter

2.1.3 Engagementer med tredjepartsudviklere, freelancere, bureauer eller offshore-teams

2.2 Politikken regulerer også enhver ekstern part, der får adgang til kildekode, testmiljøer eller CI/CD-pipelines under udviklingen.

2.3 Kravene skal håndhæves uanset kontrakttype, udviklingsmetodik eller geografisk placering for den outsourcede leverandør.

3. Mål

3.1 At håndhæve praksisser for sikker udviklingslivscyklus (SDLC) på tværs af alle outsourcede engagementer, fra planlægning til validering efter idriftsættelse.

3.2 At sikre, at alle kontrakter med eksterne udviklere indeholder obligatoriske klausuler om databeskyttelse, sikker kodning og fastholdelse af immaterielle rettigheder.

3.3 At fastlægge krav til adgangsstyring, overvågning og revision for tredjepartsudviklere, der interagerer med interne systemer.

3.4 At beskytte organisationen mod trusler i forsyningskæden, lovovertrædelser og omdømmeskade relateret til eksternt udviklet software.

3.5 At opretholde løbende efterlevelse af sikkerhedsrammeværker, herunder ISO/IEC 27001, NIST, GDPR, NIS2, DORA og COBIT 2019.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender outsourcede udviklingsprojekter med høj risiko og validerer politikundtagelser, hvor dette er begrundet.

4.1.2 Sikrer, at beslutninger om outsourcing er i overensstemmelse med strategiske målsætninger og organisationens risikovillighed.

4.2 Chief Information Security Officer (CISO)

4.2.1 Godkender leverandøronboarding ud fra et sikkerhedsperspektiv.

4.2.2 Fastlægger krav til sikkerhedskontroller for outsourcede engagementer og gennemgår hændelsesrapporter.

[... 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 mindst én gang årligt eller hyppigere under følgende omstændigheder:

9.1.1 Indførelse af nye modeller, leverandører eller jurisdiktioner for outsourcing af udvikling

9.1.2 Opdateringer af regulatoriske rammer såsom GDPR, NIS2 eller DORA

9.1.3 Efter en sikkerhedshændelse, der involverer outsourcet kode, adgang eller leverancer

9.1.4 Som led i revisionskonstateringer fra intern revision eller forbedringer i ISMS

9.2 Chief Information Security Officer (CISO) er ansvarlig for at iværksætte og koordinere gennemgangen af politikken i samråd med:

9.2.1.1 Jura og Compliance samt Indkøb (for tilpasning af kontraktuel håndhævelse)

9.2.1.2 Projekt- og produktejere (for operationel gennemførlighed)

9.2.1.3 Informationssikkerhedsteamet (for opdateringer af trusselsbillede og kontroller)

9.2.1.4 Direktionen (for endelig godkendelse)

9.3 Alle opdateringer af politikken skal:

9.3.1.1 Være versionsstyrede og opbevaret i et udpeget dokumentrepository

9.3.1.2 Kommunikeres til interessenter, der deltager i aktiviteter vedrørende outsourcet udvikling

9.3.1.3 Kobles til eventuelle opdateringer i relaterede politikker eller proceduredokumentation

9.4 En ændringslog skal ledsage hver politikversion for at sikre sporbarhed for ændringer og godkendelser.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter og understøttes af følgende relaterede dokumenter:

10.1.1 P1 - Informationssikkerhedspolitik: Fastlægger overordnede sikkerhedsprincipper for organisationen, som gælder på tværs af interne udviklingskontekster og tredjepartsudvikling.

10.1.2 P5 - Politik for ændringsstyring: Sikrer, at alle ændringer relateret til idriftsættelse fra outsourcede kodebaser gennemgås og godkendes før implementering.

10.1.3 P13 - Politik for dataklassificering og mærkning: Fastlægger, hvordan følsomme data identificeres, før de eksponeres for udviklingsleverandører eller repositories.

10.1.4 P18 - Politik for kryptografiske kontroller: Vejleder om, hvordan nøgler, hemmeligheder og følsomme legitimationsoplysninger skal håndteres under udvikling og levering.

10.1.5 P24 - Politik for sikker udvikling: Fastlægger baselinekrav for interne og eksterne praksisser for softwareudvikling.

10.1.6 P30 - Politik for hændelseshåndtering: Regulerer, hvordan brud eller sikkerhedsforhold vedrørende outsourcet udvikling eskaleres, undersøges og løses.

10.1.7 P33 - Politik for revision og overvågning af efterlevelse: Fastlægger krav til gennemgang af aktiviteter vedrørende outsourcet udvikling under revisioner eller efterlevelsesgennemgange.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset internationalt anerkendte sikkerhedsrammeværker og regler for at sikre sikker outsourcing af softwareudvikling og praksisser for leverandørstyring.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 - operationel planlægning og styring: Håndhæver proceskontroller for sikker udvikling og tredjepartsleverancer.

11.3 ISO/IEC 27002:2022 - kontroller 5.19 til 5.21, 8

11.3.1 Bilag A-kontrol 5.19 - styring af leverandørforhold: Kræver formelle aftaler med klausuler om sikkerhed og efterlevelse.

11.3.2 Bilag A-kontrol 5.20 - håndtering af informationssikkerhed i leverandøraftaler: Sikrer, at udviklingsspecifikke kontroller er indarbejdet i kontrakter.

11.3.3 Bilag A-kontrol 5.21 - styring af levering af leverandørtjenester: Omfatter overvågning af tredjepartsudviklingens leverancer og risici.

11.3.4 Bilag A-kontrol 8.27 - outsourcet udvikling: Påbyder definerede sikkerhedskrav og adgangsstyring for eksternt udviklet software.

11.3.5 Disse kontroller fastlægger strukturerede krav til udvælgelse, kontrahering og tilsyn med outsourcede udviklere, herunder praksisser for sikker udvikling, håndtering af kode og validering af leverancekvalitet.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - anskaffelsesproces: Kræver, at krav til sikker udvikling fastlægges ved anskaffelsen.

11.4.2 SA-9 - eksterne systemtjenester: Regulerer, hvordan tredjepartsudviklere sikkert interagerer med interne tjenester.

11.4.3 SA-10 - udvikleres konfigurationsstyring: Er i overensstemmelse med forpligtelser til versionsstyring, kodeadgang og ændringssporing for eksterne teams.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 28 - databehandlerforpligtelser: Kræver, at kontrakter med tredjepartsudviklere specificerer krav til sikkerhed, kontrol og revision ved håndtering af personoplysninger.

11.5.2 Artikel 32 - behandlingssikkerhed: Håndhæver passende sikkerhedsforanstaltninger (f.eks. kryptering, adgangsstyring) ved udvikling af systemer, der behandler personoplysninger.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Artikel 21(2)(a), (h), 23: Kræver, at praksisser for sikker udvikling anvendes på tværs af tredjepartsengagementer og digitale forsyningskæder med tilsyn og teknisk verifikation.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 28(1), (2): Kræver, at finansielle enheder styrer tredjepartsrisiko i IKT gennem kontraktuelle kontroller og tilsyn med sikker udvikling, særligt for kritisk outsourcet udvikling.

11.8 COBIT 2019

11.8.1 APO10 - styr leverandører: Fastlægger strukturerede krav til leverandørevaluering, kontrakter og overvågning af præstation.

11.8.2 BAI03 - styr opbygning af løsninger: Mapper direkte til sikre SDLC-processer, kodegennemgange og udviklingsvalidering.

11.8.3 DSS05 - styr sikkerhedstjenester: Er i overensstemmelse med overvågning og beskyttelse af systemer, der er udviklet eksternt eller af tredjeparter.