					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P28S					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 lovkrav

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 6.1, 8	Relevante kontroller for ISMS og leverandørforhold
ISO/IEC 27002:2022	Kontrol 5.19, 5.20, 8.25–8.27	Kontroller for leverandører og sikker udviklingslivscyklus
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Krav til anskaffelse, forsyningskæde, sikker udvikling og leverandøraftaler
EU GDPR	Artikel 28	Kontraktuelle krav og databeskyttelseskrav ved tredjepartsbehandling
EU NIS2	Artikel 21(2)(a), (h)	Kontroller for forsyningskæden og sikker applikationsudvikling
EU DORA	Artikel 10	Styring af IKT-risiko ved tredjeparter, herunder outsourcet udvikling
COBIT 2019	BAI03, DSS05	Krav til ekstern udvikling og eksterne leverandører af informationstjenester

1. Formål

1.1 Denne politik sikrer, at al outsourcet softwareudvikling – uanset om den udføres af freelancere, bureauer eller tredjepartsleverandører – gennemføres sikkert, underlagt kontraktuel styring og i overensstemmelse med gældende lovgivningsmæssige, regulatoriske og revisionsmæssige krav.

1.2 Politikken beskytter organisationen mod risici relateret til usikker kode, uklare ejerskabsforhold, dataeksponering og utilstrækkelig leverandørstyring ved at håndhæve ensartede udviklingsstandarder og tilsyn med leverandører, også hvor der ikke findes en dedikeret IT-afdeling.

1.3 Denne politik understøtter certificering efter ISO/IEC 27001:2022 ved at fastlægge tydelige forventninger til udvikling, ansvarlighed og dokumenterede kontroller for tredjepartsudviklingsaktiviteter.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle outsourcede udviklere, herunder freelancere og udviklingsbureauer

2.1.2 Alt udviklingsarbejde, der omfatter interne værktøjer, offentligt tilgængelige websites, softwareapplikationer eller automatisering af forretningsprocesser

2.1.3 Medarbejdere med ansvar for at udvælge, styre eller føre tilsyn med eksterne udviklere

2.1.4 Enhver tredjeparts systemintegration, scripting eller udvikling, der interagerer med virksomhedens data eller systemer

2.2 Politikken omfatter også enhver part eller platform med adgang til virksomhedens legitimationsoplysninger, datarepositories, kildekoderepositories, testmiljøer eller produktionssystemer.

3. Mål

3.1 Sikre, at al outsourcet udvikling følger praksis for sikker kodning, og at udviklere kontraktuelt forpligtes til at efterleve dokumenterede standarder og fortrolighedsklausuler.

3.2 Etablere ejerskab over alle leverancer – kode, aktiver, legitimationsoplysninger og dokumentation – således at alle rettigheder overdrages fuldt ud til virksomheden, og at overdragelsen kan spores ved projektets afslutning.

3.3 Forebygge almindelige udviklingsrisici, herunder genbrug af proprietær kode, forsyningskædeangreb via biblioteker, brug af frameworks uden support og ikkevurderet administratoradgang.

3.4 Kræve dokumentation før opstart for hvert outsourcet projekt, herunder kontrakter, fortrolighedsaftaler og minimumskrav til sikkerhed.

3.5 Beskytte kundedata, systemer og interne processer ved at håndhæve tæt styring af udviklingsarbejdet, test efter levering og sikker styring af systemadgang.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Godkender alle leverandørforhold og underskriver udviklingsaftaler.

4.1.2 Sikrer, at al outsourcet udvikling efterlever denne politik.

4.1.3 Fjerner adgang til virksomhedens systemer efter projektets afslutning.

4.1.4 Gennemgår dokumentation og resultater efter levering.

4.2 Projektejer (typisk intern medarbejder eller udpeget koordinator)

4.2.1 Varetager den daglige koordinering med den eksterne udvikler.

4.2.2 Verificerer, at de funktionelle krav er opfyldt, og at leverancer er testet.

4.2.3 Sikrer sikker levering af kode og legitimationsoplysninger.

4.2.4 Rapporterer udviklingsrelaterede problemer eller hændelser 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 Årlig gennemgang

9.1.1 Denne politik skal gennemgås af direktøren (GM) mindst én gang om året. Gennemgangen skal sikre, at politikken fortsat opfylder:

9.1.1.1 Kravene til ISO/IEC 27001-certificering

9.1.1.2 Ændringer i juridiske forpligtelser (f.eks. GDPR artikel 28, DORA artikel 10)

9.1.1.3 Aktuelle udviklingspraksisser og tredjepartsrisici på SMV-niveau

9.2 Løbende gennemgange

9.2.1 Gennemgang af politikken skal også ske, når:

9.2.1.1 En ny leverandør eller platform til outsourcet udvikling onboardes

9.2.1.2 Der opstår en væsentlig hændelse med relation til outsourcet udvikling

9.2.1.3 Der sker væsentlige ændringer i de anvendte værktøjer, platforme eller miljøer

9.3 Gennemgangsproces

9.3.1 Direktøren er ansvarlig for:

9.3.1.1 At verificere, at kontrakter, fortrolighedsaftaler og processer for adgangsstyring fortsat er effektive

9.3.1.2 At bekræfte, at nuværende leverandører og freelancere efterlever politikken

9.3.1.3 At revidere bestemmelser på baggrund af feedback fra tidligere projekter eller hændelser

9.4 Versionsstyring og kommunikation

9.4.1 Alle ændringer skal:

9.4.1.1 Registreres med dato, begrundelse og beskrivelse af ændringen

9.4.1.2 Godkendes af direktøren og tilføjes versionshistorikken

9.4.1.3 Kommunikeres til alle medarbejdere eller projektejere, der arbejder med eksterne udviklere

9.4.1.4 Redistribueres til alle berørte leverandører og tredjeparter, hvor det er nødvendigt

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter direkte og er afhængig af implementeringen af følgende politikker tilpasset SMV'er:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Præciserer, hvem der er ansvarlig for leverandørgodkendelse, adgangsstyring og risikoaccept ved brug af outsourcede udviklere.

10.1.2 P4S – Politik for adgangskontrol: Definerer korrekt oprettelse, begrænsning og ophør af brugerkonti og administratoradgang anvendt under outsourcet udvikling.

10.1.3 P8S – Politik for informationssikkerhedsbevidsthed og uddannelse: Sikrer, at interne medarbejdere forstår, hvordan de sikkert koordinerer med eksterne udviklere, herunder håndtering af legitimationsoplysninger og projektfiler.

10.1.4 P17S – Databeskyttelses- og privatlivspolitik: Fastlægger sikkerheds- og lovkrav for håndtering af personoplysninger, som outsourcede udviklere kan behandle i henhold til GDPR.

10.1.5 P24S – Politik for sikker udvikling: Specificerer, hvordan intern og ekstern udvikling skal følge praksis for sikker kodning samt vurdering af biblioteker og frameworks.

10.1.6 P30S – Politik for hændelseshåndtering: Kræves, når outsourcet udvikling medfører sikkerhedshændelser eller sårbarheder, og angiver rammerne for koordineret undersøgelse og afhjælpning.

10.2 Disse politikker skal implementeres parallelt for at sikre, at outsourcet udvikling ikke skaber uforvaltet risiko eller medfører brud på SMV'ers complianceforpligtelser.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Organisationer skal vurdere og behandle informationssikkerhedsrisici forbundet med leverandører.

11.1.2 Klausul 8.1 – Kræver operationel planlægning og styring, herunder tredjepartstjenester såsom outsourcet udvikling.

11.2 ISO/IEC 27002

11.2.1 Kontrol 5.19 – Anbefaler evaluering af leverandørers evne til at opfylde informationssikkerhedskrav.

11.2.2 Kontrol 5.20 – Tilskynder til regelmæssig overvågning og periodisk gennemgang af tredjepartstjenester.

11.2.3 Kontrol 8.25–8.27 – Beskriver praksis for sikker udviklingslivscyklus, der er relevante for outsourcet udvikling.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-4 – Kræver, at anskaffelsesstrategier omfatter informationssikkerhedsforanstaltninger.

11.3.2 SA-9 – Omhandler ekstern systemudvikling og risici i forsyningskæden.

11.3.3 SA-11 – Definerer sikker udviklingspraksis, herunder kodegennemgang og afhjælpning af fejl.

11.3.4 SA-15 – Tilskynder til anvendelse af automatiserede værktøjer til fejldetektion og software assurance.

11.3.5 SR-3 – Kræver, at leverandøraftaler omfatter cybersikkerhedskrav.

11.4 EU's generelle forordning om databeskyttelse (GDPR)

11.4.1 Artikel 28 – Kræver kontrakter med tredjepartsdatabehandlere, der sikrer passende databeskyttelsesforanstaltninger, og er direkte relevant for udviklere, der behandler eller har adgang til personoplysninger.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(a), (h) – Kræver kontroller for sikkerhed i forsyningskæden og sikker softwareudviklingspraksis for omfattede digitale tjenesteudbydere, herunder SMV'er, hvor relevant.

11.6 EU Digital Operational Resilience Act (DORA)

11.6.1 Artikel 10 – Kræver styring af IKT-risiko ved tredjeparter, herunder udviklingsaftaler, sikkerhedsforpligtelser og risikokontroller relateret til tredjepartsleverandører.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build – Sikrer, at ekstern udvikling opfylder forretningskrav og sikkerhedsforventninger.

11.7.2 DSS05 – Manage Security Services – Kræver, at eksterne sikkerhedstjenester og udviklingsleverandører arbejder under håndhævede sikkerhedsregler og tilsyn.