					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P37S					Dokumenttitel: **Politik for juridisk og regulatorisk compliance**						
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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrol 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
EU GDPR	Artikel 5, 6, 32, 33	
EU NIS2	Artikel 21(2)(a), 21(2)(f), 23	
EU DORA	Artikel 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Formål

1.1 Denne politik fastlægger organisationens tilgang til at identificere, efterleve og dokumentere overholdelse af juridiske, regulatoriske og kontraktuelle forpligtelser.

1.2 Den fastlægger tydelige ansvarsområder og praktiske tiltag, som hjælper virksomheden med at opfylde sine complianceforpligtelser, herunder databeskyttelseslovgivning, cybersikkerhedsrammeværk, kundeaftaler og certificeringskrav.

1.3 Den sikrer, at virksomheden også uden et særskilt complianceteam kan opretholde juridisk forsvarlig drift, reagere korrekt på hændelser og bevare fuldt revisionsberedskab.

1.4 Denne politik er væsentlig for at understøtte certificering efter ISO/IEC 27001:2022 og for at opfylde eksterne forventninger fra kunder, tilsynsmyndigheder og partnere.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, kontrahenter, freelancere og tredjepartsleverandører.

2.1.2 Alle tjenester, driftsaktiviteter, systemer og datahåndteringsaktiviteter, hvor organisationen skal opfylde juridiske eller kontraktuelle krav.

2.1.3 Alle lokationer og enheder, der anvendes til behandling af forretningsoplysninger, uanset om de er kontorbaserede, anvendes til fjernarbejde eller er cloudhostede.

2.2 Politikken omfatter:

2.2.1 Databeskyttelseslovgivning såsom EU GDPR.

2.2.2 Cybersikkerhedsregulering såsom EU NIS2.

2.2.3 Sektorspecifikke forpligtelser, hvor det er relevant.

2.2.4 Kundekontrakter, fortrolighedsaftaler og klausuler om revisionsret.

2.2.5 Frivillige certificeringer, f.eks. ISO 27001, og interne politikker, som skal håndhæves for at sikre overholdelse.

3. Mål

3.1 Etablere ansvarlighed: Tildele klart ansvar for overvågning, opdatering og håndhævelse af juridiske, regulatoriske og kontraktuelle forpligtelser.

3.2 Beskytte virksomheden: Minimere risikoen for lovovertrædelser, bøder, brud på persondatasikkerheden og omdømmeskade.

3.3 Understøtte revisionsberedskab: Opretholde verificerbare registreringer, der dokumenterer, hvordan organisationen opfylder sine complianceforpligtelser.

3.4 Understøtte integration i politikker: Sikre, at juridiske og regulatoriske forpligtelser håndhæves konsekvent på tværs af alle politikker og processer.

3.5 Håndtere undtagelser transparent: Sikre, at eventuelle undtagelser fra compliancekrav dokumenteres, begrundes og godkendes for at reducere ansvarseksponering.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for organisationens juridiske og regulatoriske compliance.

4.1.2 Vedligeholder complianceregistret og sikrer, at det holdes opdateret.

4.1.3 Gennemgår kundekontrakter og sikrer, at specifikke forpligtelser registreres og håndhæves.

4.1.4 Godkender kun undtagelser fra complianceforpligtelser, når de er juridisk forsvarlige og ledsages af kompenserende kontroller.

4.2 Eksterne rådgivere, f.eks. juridiske rådgivere, IT-rådgivere eller compliancekonsulenter

4.2.1 Understøtter direktøren med at identificere gældende lovkrav, certificeringer og forpligtelser, f.eks. GDPR, NIS2 og ISO 27001.

4.2.2 Yder rådgivning om fortolkning af nye regler eller ændringer i eksisterende lovgivning.

4.2.3 Kan bistå ved opdatering af politikker, revisioner eller håndtering af brud, når der foreligger juridisk eksponering.

[... 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 Planlagt årlig gennemgang

9.1.1 Denne politik skal gennemgås hver 12. måned af direktøren.

9.1.2 Gennemgangen skal bekræfte:

9.1.2.1 Relevans i forhold til den aktuelle juridiske og kontraktuelle kontekst.

9.1.2.2 Korrekt afspejling af kundeaftaler og serviceforpligtelser.

9.1.2.3 Overensstemmelse med complianceregistret og øvrige politikker.

9.2 Hændelsesudløste opdateringer

9.2.1 Øjeblikkelig gennemgang kræves, hvis:

9.2.1.1 En ny lov eller regulering bliver gældende, f.eks. en ny databeskyttelsesregel.

9.2.1.2 En kunde tilføjer komplekse compliancevilkår til sin aftale.

9.2.1.3 Der opstår et brud eller en compliancehændelse.

9.2.1.4 Virksomheden udvider til et reguleret marked eller en reguleret sektor.

9.3 Godkendelse af opdateringer og versionsstyring

9.3.1 Alle opdateringer skal dokumenteres, versionsstyres og godkendes af direktøren.

9.3.2 Historiske versioner skal opbevares af hensyn til revision og juridiske formål.

9.4 Kommunikation af ændringer

9.4.1 Medarbejdere og kontrahenter skal informeres om ændringer i politikken inden for 5 arbejdsdage efter godkendelse.

9.4.2 Berørte leverandører skal også bekræfte opdaterede vilkår, før leveringen af tjenesten fortsætter.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøttes og håndhæves gennem følgende SME-politikker:

10.1.1 P3S – Politik for acceptabel brug: Forebygger adfærd, som kan overtræde juridiske eller kontraktuelle vilkår, f.eks. uautoriseret fildeling.

10.1.2 P8S – Politik for bevidstgørelse om informationssikkerhed og uddannelse: Uddanner medarbejdere i complianceforpligtelser og i, hvordan overtrædelser undgås.

10.1.3 P14S – Politik for dataopbevaring og bortskaffelse: Sikrer lovlige datahåndteringspraksisser på tværs af dataenes livscyklus.

10.1.4 P17S – Politik for databeskyttelse og privatliv: Opfylder GDPR og kundekrav til datahåndtering.

10.1.5 P30S – Politik for hændelseshåndtering: Beskriver, hvordan brud på persondatasikkerheden eller manglende compliance skal håndteres, herunder underretningsfrister.

10.1.6 P36S – Politik for sociale medier og ekstern kommunikation: Sikrer, at offentlig kommunikation ikke overtræder juridiske eller regulatoriske forpligtelser.

10.2 Hver tilknyttet politik håndhæver en del af rammen for juridisk compliance og skal anvendes samlet.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Handlinger til håndtering af risici og muligheder: Omfatter compliancerisici.

11.1.2 Klausul 8.1 – Operationel planlægning og styring: Kræver gennemførelse af processer, der opfylder juridiske og kontraktuelle krav.

11.2 ISO/IEC 27002

11.2.1 Kontrol 5.36 – Vejleder organisationen i at opretholde registreringer af forpligtelser og sikre passende respons på juridiske og regulatoriske behov.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politikker og procedurer: Kræver formelle politikker for compliance.

11.3.2 PM-1 – Plan for informationssikkerhedsprogram: Kræver integration af juridisk compliance i sikkerhedsplanlægningen.

11.3.3 CA-1 – Vurdering, autorisation og overvågning.

11.3.4 AU-1 – Revisionspolitik: Kræver vedligeholdelse af dokumentation for compliance.

11.4 EU GDPR

11.4.1 Artikel 5 – Principper for behandling af oplysninger, herunder ansvarlighed.

11.4.2 Artikel 6 – Behandlingsgrundlag.

11.4.3 Artikel 32 – Behandlingssikkerhed.

11.4.4 Artikel 33 – Underretning om brud inden for 72 timer.

11.5 EU NIS2-direktivet

11.5.1 Artikel 21(2)(a) og (f) – Interne politikker for risiko- og regulatorisk kontrol.

11.5.2 Artikel 23 – Håndhævelse og sanktioner ved manglende compliance.

11.6 EU DORA-forordningen

11.6.1 Artikel 5(2) – Tilsyn med styring af IKT-risiko.

11.6.2 Artikel 9(1) – Intern styring af compliance.

11.6.3 Artikel 17 – Kontraktuelle ordninger med IKT-tjenesteudbydere.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: Sikrer, at compliancerisici spores og håndteres.

11.7.2 APO13 – Managed Security: Omfatter risikobaseret håndhævelse af regulatorisk og kontraktuel compliance.

11.7.3 DSS01 – Managed Operations: Kræver driftsmæssig parathed til at opfylde juridiske forpligtelser.