					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P37S					Dokumenttitel: **Policy för rättslig och regulatorisk regelefterlevnad**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

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

1. Syfte

1.1 Denna policy fastställer organisationens arbetssätt för att identifiera, uppfylla och kunna påvisa efterlevnad av rättsliga, regulatoriska och avtalsmässiga skyldigheter.

1.2 Den anger tydliga roller och ansvar samt praktiska åtgärder som hjälper verksamheten att uppfylla sina regelefterlevnadskrav, inklusive dataskyddslagstiftning, cybersäkerhetsramverk, kundavtal och certifieringskrav.

1.3 Den säkerställer att verksamheten, även utan en särskild regelefterlevnadsfunktion, kan bedriva rättsenlig verksamhet, hantera incidenter på ett ändamålsenligt sätt och upprätthålla revisionsberedskap.

1.4 Denna policy är väsentlig för att möjliggöra certifiering enligt ISO/IEC 27001:2022 och för att uppfylla externa förväntningar från kunder, tillsynsmyndigheter och partner.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 alla anställda, entreprenörer, frilansare och tredjepartsleverantörer

2.1.2 alla tjänster, verksamheter, system och datahanteringsrutiner där organisationen måste uppfylla rättsliga krav eller avtalskrav

2.1.3 alla platser och miljöer som används för att behandla verksamhetsinformation, oavsett om det sker på kontor, vid distansarbete eller i molnmiljö

2.2 Policyn omfattar:

2.2.1 dataskyddslagstiftning såsom EU:s GDPR

2.2.2 cybersäkerhetsregelverk såsom EU:s NIS2-direktiv

2.2.3 sektorsspecifika skyldigheter, där tillämpligt

2.2.4 kundavtal, sekretessavtal (NDA) och revisionsklausuler

2.2.5 frivilliga certifieringar, till exempel ISO 27001, samt interna policyer som måste tillämpas för att uppnå efterlevnad

3. Mål

3.1 Fastställa ansvarsskyldighet: tilldela tydligt ansvar för övervakning, uppdatering och tillämpning av rättsliga, regulatoriska och avtalsmässiga skyldigheter.

3.2 Skydda verksamheten: minimera risken för lagöverträdelser, sanktionsavgifter, personuppgiftsincidenter och anseendeskada.

3.3 Möjliggöra revisionsberedskap: upprätthålla verifierbara underlag som visar hur organisationen uppfyller sina regelefterlevnadskrav.

3.4 Stödja policyintegration: säkerställa att rättsliga och regulatoriska skyldigheter tillämpas konsekvent i alla policyer och processer.

3.5 Hantera undantag transparent: säkerställa att undantag från regelefterlevnadskrav dokumenteras, motiveras och godkänns för att minska ansvarsrisker.

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Har det övergripande ansvaret för organisationens rättsliga och regulatoriska regelefterlevnad.

4.1.2 Upprätthåller registret över regelefterlevnadskrav och säkerställer att det hålls uppdaterat.

4.1.3 Granskar kundavtal och säkerställer att specifika skyldigheter följs upp och tillämpas.

4.1.4 Godkänner undantag från regelefterlevnadskrav endast när detta är rättsligt motiverat och kompenserande kontroller finns.

4.2 Externa rådgivare (t.ex. juridiska rådgivare, IT- eller compliancekonsulter)

4.2.1 Stödjer GM genom att identifiera tillämpliga lagar, certifieringar och skyldigheter, till exempel GDPR, NIS2 och ISO 27001.

4.2.2 Ger vägledning om tolkningen av nya regelverk eller ändringar i befintlig lagstiftning.

4.2.3 Kan bistå vid policyuppdateringar, revisioner eller incidenthantering när det finns rättslig exponering.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Planerad årlig granskning

9.1.1 Denna policy ska granskas var tolfte månad av GM.

9.1.2 Granskningen ska bekräfta:

9.1.2.1 att policyn är relevant utifrån gällande rättslig och avtalsmässig kontext

9.1.2.2 att kundavtal och tjänsteåtaganden återspeglas korrekt

9.1.2.3 att policyn är anpassad till registret över regelefterlevnadskrav och övriga policyer

9.2 Händelsestyrda uppdateringar

9.2.1 Omedelbar granskning krävs om:

9.2.1.1 en ny lag eller reglering blir tillämplig, till exempel en ny dataskyddsregel

9.2.1.2 en kund lägger till komplexa regelefterlevnadskrav i sitt avtal

9.2.1.3 en incident eller överträdelse av efterlevnadskrav inträffar

9.2.1.4 organisationen expanderar till en reglerad marknad eller sektor

9.3 Godkännande av uppdateringar och versionshantering

9.3.1 Alla uppdateringar ska dokumenteras, versionshanteras och godkännas av GM.

9.3.2 Historiska versioner ska bevaras för revisions- och rättsliga ändamål.

9.4 Kommunikation av förändringar

9.4.1 Anställda, entreprenörer och tredjepartsleverantörer ska informeras om policyändringar inom fem arbetsdagar från godkännande.

9.4.2 Berörda leverantörer ska också bekräfta uppdaterade villkor innan fortsatt tjänsteleverans.

10. Relaterade policyer och kopplingar

10.1 Denna policy stöds och tillämpas genom följande SME-policyer:

10.1.1 P3S – Policy för godtagbar användning: förebygger beteenden som kan strida mot rättsliga eller avtalsmässiga villkor, till exempel otillåten fildelning

10.1.2 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: utbildar personal om regelefterlevnadskrav och hur överträdelser undviks

10.1.3 P14S – Policy för databevarande och bortskaffning: säkerställer laglig datahanteringspraxis genom hela informationslivscykeln

10.1.4 P17S – Policy för dataskydd och integritet: uppfyller krav enligt GDPR och krav för hantering av kunddata

10.1.5 P30S – Policy för incidenthantering: beskriver hur personuppgiftsincidenter eller brister i efterlevnad ska hanteras, inklusive tidsfrister för incidentanmälan

10.1.6 P36S – Policy för sociala medier och extern kommunikation: säkerställer att extern kommunikation inte bryter mot rättsliga eller regulatoriska skyldigheter

10.2 Varje länkad policy genomför en del av ramverket för rättslig och regulatorisk regelefterlevnad och ska tillämpas samordnat.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.1 – Åtgärder för att hantera risker och möjligheter: omfattar risker kopplade till regelefterlevnad.

11.1.2 Klausul 8.1 – Operativ planering och styrning: kräver att processer genomförs så att rättsliga krav och avtalskrav uppfylls.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.36 – vägleder organisationen i att upprätthålla underlag om skyldigheter och säkerställa ändamålsenlig hantering av rättsliga och regulatoriska krav.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Policy and Procedures: kräver formella policyer för regelefterlevnad.

11.3.2 PM-1 – Information Security Program Plan: kräver att rättslig regelefterlevnad integreras i säkerhetsplaneringen.

11.3.3 CA-1 – Assessment, Authorization, and Monitoring.

11.3.4 AU-1 – Audit Policy: kräver att underlag för regelefterlevnad upprätthålls.

11.4 EU:s GDPR

11.4.1 Artikel 5 – principer för behandling av personuppgifter, inklusive ansvarsskyldighet

11.4.2 Artikel 6 – rättslig grund för behandling

11.4.3 Artikel 32 – säkerhet i samband med behandling

11.4.4 Artikel 33 – anmälan av personuppgiftsincidenter inom 72 timmar

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(a) och (f) – interna policyer för riskhantering och regulatorisk styrning

11.5.2 Artikel 23 – tillämpning och sanktioner vid bristande efterlevnad

11.6 EU:s DORA-förordning

11.6.1 Artikel 5(2) – tillsyn över IKT-riskhantering

11.6.2 Artikel 9(1) – intern styrning av regelefterlevnad

11.6.3 Artikel 17 – avtalsarrangemang med IKT-tjänsteleverantörer

11.7 COBIT 2019

11.7.1 APO12 – Hantera risk: säkerställer att risker kopplade till regelefterlevnad följs upp och hanteras.

11.7.2 APO13 – Hantera säkerhet: omfattar riskbaserad tillämpning av regulatorisk och avtalsmässig efterlevnad.

11.7.3 DSS01 – Hantera drift: kräver operativ beredskap för att uppfylla rättsliga skyldigheter.