					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P37					Dokumenttitel: **Policy för rättslig och regulatorisk efterlevnad**							
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**

1. Syfte

1.1 Denna policy fastställer det obligatoriska ramverket för att identifiera, hantera och uppfylla alla rättsliga, regulatoriska och avtalsmässiga skyldigheter som är relevanta för organisationens informationssäkerhet, dataskydd och operativa verksamhet.

1.2 Syftet är att förebygga bristande efterlevnad som kan leda till sanktionsavgifter, rättsligt ansvar, verksamhetsstörningar, anseendeskada eller tillsynsåtgärder.

1.3 Denna policy stöder integreringen av regelefterlevnadskrav i styrning, riskhantering, operativa arbetsflöden, projektlivscykler och systemutformning.

1.4 Den säkerställer att alla relevanta skyldigheter – över olika jurisdiktioner, branscher och regulatoriska tillämpningsområden – dokumenteras tydligt, bedöms, övervakas och efterlevs inom organisationen.

2. Omfattning

2.1 Denna policy gäller för alla avdelningar, funktioner, affärsenheter och personer som agerar på organisationens vägnar, inklusive:

2.1.1 Tillsvidareanställda och visstidsanställda

2.1.2 Entreprenörer, konsulter och praktikanter

2.1.3 Tredjepartsleverantörer, personuppgiftsbiträden eller partner som hanterar organisationens data, system eller regulatoriska ansvar

2.1.4 Alla verksamhetsprocesser, projekt eller initiativ som omfattas av rättsliga eller regulatoriska krav

2.2 Områden för regelefterlevnad som omfattas av denna policy inkluderar bland annat:

2.2.1 Krav inom informationssäkerhet och cybersäkerhet (t.ex. ISO/IEC 27001, NIS2, DORA)

2.2.2 Dataskydds- och integritetslagstiftning (t.ex. GDPR, branschspecifik integritetslagstiftning)

2.2.3 Sektorsspecifika regelverk (t.ex. finansiell verksamhet, medicinteknik, fordonsindustri, försvar)

2.2.4 Avtalsmässiga skyldigheter enligt sekretessavtal (NDA), servicenivåavtal (SLA) eller avtal om tredjepartsbehandling av data

2.2.5 Rättsliga krav avseende incidentrapportering, kontakter med brottsbekämpande myndigheter och internationella dataöverföringar

3. Mål

3.1 Att säkerställa att alla tillämpliga lagar, regelverk, standarder och avtalsmässiga skyldigheter identifieras, dokumenteras, tolkas och tillämpas i hela organisationen.

3.2 Att integrera rättsliga och regulatoriska krav i organisationens ISMS, riskhanteringsprocesser, leverantörsavtal samt i utformningen av produkter och tjänster.

3.3 Att tillhandahålla en mekanism för proaktiv övervakning av regulatoriska förändringar samt för att uppdatera kontroller och dokumentation i enlighet med dessa.

3.4 Att definiera tydligt ansvar för tillsyn av efterlevnad, eskalering av överträdelser, undantagshantering och extern rapportering.

3.5 Att säkerställa revisionsbarhet och försvarbarhet i organisationens rättsliga och regulatoriska ställning vid inspektioner, utredningar eller certifieringsgranskningar.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Har det övergripande strategiska ansvaret för rättslig och regulatorisk efterlevnad i hela organisationen.

4.1.2 Granskar och godkänner beslut om regelefterlevnad med hög risk, inklusive riskacceptanser och rättsliga tvister.

4.2 Complianceansvarig / chefsjurist / bolagsjurist

4.2.1 Upprätthåller registret över regelefterlevnadskrav med samtliga tillämpliga lagar, standarder, certifieringar och avtalsklausuler.

4.2.2 Genomför rättsliga konsekvensbedömningar för nya tjänster, marknader eller dataflöden.

4.2.3 Tillhandahåller auktoritativ tolkning av lagar och standarder.

[... 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 Årlig policygranskning

9.1.1 Denna policy ska granskas minst en gång per kalenderår för att:

9.1.1.1 Säkerställa fortsatt anpassning till uppdaterade lagar, branschstandarder och regulatoriska ramverk

9.1.1.2 Validera operativ effektivitet baserat på revisionsiakttagelser och incidenthistorik

9.1.1.3 Återspegla organisatoriska förändringar (t.ex. nya jurisdiktioner, system eller verksamhetsområden)

9.2 Händelsestyrda granskningar

9.2.1 Interimistiska granskningar ska initieras när:

9.2.2 Ett nytt rättsligt eller regulatoriskt krav införs eller uppdateras

9.2.3 En efterlevnadsincident eller revision visar på brister i policyn

9.2.4 Organisationen går in på en ny marknad eller ett nytt tjänsteområde som omfattas av särskilda regelverk

9.2.5 Trender i tillsynsåtgärder eller vägledning från tillsynsmyndigheter indikerar förändringar i riskläget

9.3 Ägarskap och godkännande

9.3.1 Juridikfunktionen och complianceansvarig har gemensamt ansvar för att samordna granskningsprocessen.

9.3.2 Slutliga revideringar av policyn ska godkännas av verkställande ledning och loggas i registret över policyändringar, tillsammans med tillhörande referenser till ändringsstyrning och kommunikationsplaner.

9.4 Versionshantering och kommunikation

9.4.1 Varje uppdaterad version av denna policy ska:

9.4.1.1 Innehålla en sammanfattning av de viktigaste ändringarna

9.4.1.2 Distribueras på nytt genom officiella kanaler (t.ex. policyportal, LMS, interna nyhetsbrev)

9.4.1.3 Kräva bekräftelse från berörd personal, särskilt personer inom juridik, drift, säkerhet och leverantörsstyrning

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med och förstärker följande policyer inom organisationens ISMS:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer de grundläggande styrningsprinciperna som säkerställer att alla informationssäkerhetspolicyer – inklusive regelefterlevnad – är anpassade till strategiska verksamhetskrav och regulatoriska krav.

10.1.2 P2 – Policy för styrningsroller och ansvar: Definierar beslutsbefogenheter, inklusive juridiska roller och roller inom regelefterlevnad med ansvar för regulatorisk tillsyn och ansvarsskyldighet.

10.1.3 P6 – Riskhanteringspolicy: Stödjer utvärdering, ägarskap och riskreducering av rättsliga och regulatoriska risker kopplade till regelefterlevnad i hela organisationen.

10.1.4 P8 – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer att all personal känner till sina skyldigheter avseende regelefterlevnad och får utbildning som är anpassad till rollen.

10.1.5 P12 – Policy för tillgångshantering: Förstärker rättsliga skyldigheter avseende hantering och skydd av reglerade eller avtalsstyrda tillgångar, inklusive sådana som omfattar personuppgifter och kritisk infrastruktur.

10.1.6 P30 – Policy för incidenthantering: Styr obligatoriska rättsliga anmälningar (t.ex. artikel 33 i GDPR) och eskaleringsrutiner vid en efterlevnadsöverträdelse eller regulatorisk händelse.

10.1.7 P33 – Policy för revision och övervakning av regelefterlevnad: Tillhandahåller strukturerade granskningsaktiviteter – inklusive kontrolltestning och insamling av bevismaterial – som krävs för intern och extern verifiering av regelefterlevnad.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 4.2 – Förstå intressenters behov och förväntningar: Kräver att rättsliga och regulatoriska krav identifieras och integreras i ISMS.

11.1.2 Klausul 5.1 – Ledarskap och åtagande: Kräver ansvar på ledningsnivå för att etablera och upprätthålla rättslig efterlevnad i hela organisationen.

11.1.3 Klausul 5.3 – Organisatoriska roller, ansvar och befogenheter: Säkerställer tydlighet i roller för rättslig tillsyn och regulatorisk efterlevnad.

11.1.4 Bilaga A, kontroll 5.36 – Efterlevnad av rättsliga krav, författningskrav och avtalskrav: Fastställer kravet att identifiera och uppfylla skyldigheter som följer av lagar, regelverk och avtal.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.36: Ger vägledning för genomförande av ett register över regelefterlevnadskrav, validering av regulatoriska krav och säkerställande av strukturerat bevarande av bevismaterial.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Policy och rutiner för säkerhetsplanering: Kräver att regelefterlevnadskrav byggs in i styrningsstrukturer och dokumentation.

11.3.2 PM-1 – Plan för informationssäkerhetsprogram: Kräver regulatoriska kontroller som en del av det bredare säkerhetsprogrammet.

11.3.3 CA-7 – Kontinuerlig övervakning: Stödjer övervakning av kontrolleffektivitet för att uppfylla rättsliga krav och policykrav.

11.3.4 AU-9 – Skydd av revisionsinformation: Säkerställer att revisionsloggar och registreringar för regelefterlevnad skyddas och finns tillgängliga för granskning.

11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 5 – Principer för behandling av personuppgifter: Kräver laglig behandling, transparens och ansvarsskyldighet.

11.4.2 Artikel 6 – Laglighet i behandlingen: Kräver lämplig rättslig grund för all behandling av personuppgifter.

11.4.3 Artikel 24 – Den personuppgiftsansvariges ansvar: Fastställer direkt ansvarsskyldighet för att säkerställa regulatorisk efterlevnad.

11.4.4 Artikel 32 – Säkerhet i samband med behandling: Kräver genomförande av lämpliga tekniska och organisatoriska åtgärder.

11.4.5 Artikel 33 – Anmälan av personuppgiftsincidenter: Kräver att personuppgiftsincidenter rapporteras till relevanta myndigheter inom 72 timmar.

11.5 EU:s NIS2-direktiv (2022/2555)

11.5.1 Artiklarna 20–21: Kräver att väsentliga och viktiga entiteter genomför dokumenterad styrning, strategier för rättslig efterlevnad och kontinuerlig granskning av rättsliga risker.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 5.2 – Ramverk för IKT-riskhantering: Kräver att rättslig efterlevnad integreras i bredare riskhanterings- och tillsynsfunktioner.

11.6.2 Artikel 19 – Risker kopplade till IKT-tredjepartsleverantörer: Ställer särskilda rättsliga krav på hantering av avtalsmässiga och regulatoriska skyldigheter som involverar externa leverantörer och plattformar.

11.7 COBIT 2019

11.7.1 APO12 – Hantera risk: Inkluderar rättslig och regulatorisk efterlevnad som kritiska delar av organisationens riskstyrning.

11.7.2 MEA03 – Övervaka efterlevnad av externa krav: Definierar löpande övervakning, undantagshantering och revisionsberedskap för alla typer av regulatoriska skyldigheter.