					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P27					Dokumenttitel: **Policy för användning av molntjänster**							
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 8	Krav på operativ planering och styrning av molntjänster.
ISO/IEC 27002:2022	Kontroller 5.23–5.25	Krav avseende användning, policy och säkerhet för molntjänster.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Användning av externa system, avtalsmässiga och tekniska krav, kryptografiska skydd samt skydd i leveranskedjan.
EU:s GDPR	Artiklarna 28, 32, kapitel V	Krav för personuppgiftsbiträden i molnmiljöer, säkerhet i behandlingen samt dataöverföringar.
EU:s NIS2-direktiv	Artikel 21(2)(f, i)	Krav avseende tredjepartsrisker och leveranskedjan.
EU:s DORA-förordning	Artiklarna 5(2), 28	Styrning av IKT och tredjepartsleverantörer (molntjänster) för finansiella entiteter.
COBIT 2019	BAI04, DSS01, DSS05	Tillgänglighet, drift och säkerhetshantering för molntjänster.

1. Syfte

1.1 Denna policy fastställer organisationens obligatoriska krav för säker, regelriktig och ansvarsfull användning av molntjänster inom leveransmodellerna Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) och Software-as-a-Service (SaaS).

1.2 Policyn syftar till att säkerställa att molntjänster införs och styrs på ett sätt som skyddar informationstillgångars konfidentialitet, riktighet och tillgänglighet samt uppfyller regulatoriska, rättsliga och avtalsmässiga krav.

1.3 Den definierar kontroller för att hantera molnrisker, skydda data, följa upp leverantörers efterlevnad och förhindra otillåten användning. Den stödjer även verksamhetsinnovation genom molnplattformar genom att förena säkerhet, driftsäkerhet och kostnadseffektivitet.

2. Omfattning

2.1 Denna policy gäller för alla anställda, entreprenörer, tredjepartsleverantörer och externa konsulter som tilldelar, konfigurerar, får åtkomst till, administrerar eller använder molntjänster för organisationens räkning.

2.2 Den gäller för alla miljöer där organisationens data eller arbetslaster behandlas, inklusive:

2.2.1 publika, privata, hybrida och community-moln

2.2.2 alla modeller för molntjänster (IaaS, PaaS, SaaS)

2.2.3 multicloud- och federerade arkitekturer

2.2.4 användning av skugg-IT eller personliga molnkonton för verksamhetsändamål

2.3 Den omfattar alla dataklassificeringar och gäller såväl interna system som leverantörsdrivna plattformar där organisationens data eller reglerade data lagras eller behandlas.

3. Mål

3.1 Att säkerställa säker och enhetlig användning av molnteknik genom tydligt definierade användningsregler, säkerhetsbaslinjer och styrningsroller.

3.2 Att minimera operativa och regulatoriska risker kopplade till molntjänster, inklusive obehörig åtkomst, personuppgiftsincidenter, felkonfiguration, bristande efterlevnad och tjänsteavbrott.

3.3 Att säkerställa säkerhets- och dataskyddskrav för alla molnleverantörer och verifiera efterlevnad genom avtalsklausuler, bedömningar och revisionsrätt.

3.4 Att möjliggöra skalbar och resilient användning av molntjänster utan att äventyra säkerhetsnivå, rättsliga krav eller verksamhetskontinuitet.

3.5 Att anpassa styrning och användning av molntjänster till organisationens ISMS, rättsliga skyldigheter (t.ex. GDPR och DORA), sektorsspecifika riktlinjer och erkänd branschpraxis (t.ex. NIST och COBIT).

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner policyn för användning av molntjänster och den strategiska färdplanen för införande av molntjänster.

4.1.2 Granskar och godkänner undantag med hög risk från standardiserade styrningskrav för molntjänster.

4.1.3 Säkerställer att molninitiativ får tillräcklig finansiering, styrning och integration med organisationens ramverk för riskhantering.

4.2 Informationssäkerhetschef (CISO)

4.2.1 Är policyägare för denna policy och för organisationens register över molntjänster.

4.2.2 Godkänner onboarding av nya molnleverantörer baserat på leverantörsgranskning och riskbedömning.

4.2.3 Granskar leverantörers dokumentation avseende regelefterlevnad och validerar säkerhetsmässig anpassning.

[... 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 Denna policy ska granskas minst årligen och uppdateras vid behov för att säkerställa fortsatt anpassning till:

9.1.1 förändrade rättsliga och regulatoriska krav (t.ex. GDPR, NIS2, DORA)

9.1.2 ändringar i standarderna ISO/IEC 27001 eller ISO/IEC 27002

9.1.3 uppdateringar av organisationens molnarkitektur, hotlandskap eller tjänsteportfölj

9.1.4 incidentutredningar, revisionsresultat eller erfarenheter från operativ användning

9.2 CISO ansvarar för att initiera granskningen och sammankalla relevanta intressenter, inklusive:

9.2.1 molnsäkerhetsarkitekt

9.2.2 juridik- och regelefterlevnadsteam

9.2.3 upphandling och leverantörsansvariga

9.2.4 tjänsteägare och IT-drift

9.3 Alla uppdateringar ska:

9.3.1 versionshanteras och dateras

9.3.2 godkännas av verkställande ledning

9.3.3 kommuniceras till berörda parter, inklusive anställda, entreprenörer och tredje part

9.3.4 arkiveras enligt interna regler för dokumentation

9.4 Interimistiska granskningar kan utlösas av:

9.4.1 nya engagemang med CSP eller större migreringar

9.4.2 nya hot mot molninfrastruktur

9.4.3 väsentliga förändringar i avtalsmässiga, rättsliga eller sektorsspecifika skyldigheter

10. Relaterade policyer och kopplingar

10.1 Denna policy är nära kopplad till och beroende av följande interna policyer:

10.1.1 P1 – Informationssäkerhetspolicy: Fastställer övergripande principer för säker drift av system och tjänster, vilka denna policy tillämpar i molnkontext.

10.1.2 P5 – Ändringshanteringspolicy: Alla ändringar i molnkonfigurationer ska följa rutinerna för ändringsstyrning som anges i P5.

10.1.3 P13 – Policy för dataklassificering och märkning: Anger hur data ska bedömas före överföring till molntjänster och hur kontroller såsom kryptering och datalokalitet ska tillämpas.

10.1.4 P18 – Policy för kryptografiska kontroller: Tillhandahåller standarder för kryptering, nyckelhantering och användning av kryptografiska algoritmer som direkt ska tillämpas i konfigurationer för molntjänster.

10.1.5 P22 – Loggnings- och övervakningspolicy: Anger krav för insamling, bevarande och analys av loggar som ska upprätthållas i molnmiljöer.

10.1.6 P30 – Policy för incidenthantering: Definierar rutiner för eskalering, begränsning och åtgärdande av molnrelaterade säkerhetshändelser.

10.1.7 P33 – Policy för övervakning av revision och regelefterlevnad: Stödjer revisionsberedskap och kontinuerlig säkerställning av att molnkontroller tillämpas och följs upp.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001: Klausul 8.1 – operativ planering och styrning: Kräver att organisationer inför och styr de processer som behövs för att uppfylla informationssäkerhetskrav, inklusive processer som omfattar molnmiljöer.

11.2 ISO/IEC 27002:2022 – kontroller 5.23 till 5.25:

11.2.1 Bilaga A Kontroll 5.23 – användning av molntjänster: Kräver riskbaserad bedömning, formellt godkännande och dokumentation av användning av molntjänster.

11.2.2 Bilaga A Kontroll 5.24 – policy för användning av molntjänster: Kräver att formella policyer för användning av molntjänster etableras och tillämpas i linje med organisationens behov och risker.

11.2.3 Bilaga A Kontroll 5.25 – säkerhet i molntjänster: Kräver integration av säkerhet, avtalsmässiga skydd och övervakning av arbetslaster och data i molnmiljöer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – användning av externa system: Kräver definierade regler och villkor för åtkomst till organisationens resurser från externa eller molnbaserade system.

11.3.2 SA-9(5) – externa informationssystemtjänster: Kräver avtalsmässiga säkerhetskrav, styrning och kontinuerlig övervakning för tredjepartsbaserade molnsystem.

11.3.3 SC-12 till SC-28 – kryptografiska skydd, gränsskydd och överföringsintegritet: Stämmer överens med krav på kryptering, identitets- och åtkomsthantering för tjänster i molnmiljö och data under överföring.

11.3.4 SR-5 – skydd i leveranskedjan: Stödjer granskning och avtalsstyrning av CSP:er som deltar i tjänsteleveransen.

11.4 EU:s GDPR (2016/679):

11.4.1 Artikel 28 – skyldigheter för personuppgiftsbiträden: Kräver formella avtal med molnleverantörer för att säkerställa säkerhet, konfidentialitet och revisionsbarhet vid behandling av personuppgifter.

11.4.2 Artikel 32 – säkerhet i behandlingen: Stödjer tillämpning av kryptering, åtkomstkontroller, loggning och andra skyddsåtgärder i molnmiljöer.

11.4.3 Kapitel V – internationella dataöverföringar: Kräver laglig överföring av data utanför EU/EES med hjälp av skyddsåtgärder såsom SCC eller beslut om adekvat skyddsnivå.

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

11.5.1 Artikel 21(2)(f, i): Kräver att entiteter hanterar risker från tredjepartsleverantörer av molntjänster och säkerställer den digitala leveranskedjans integritet genom avtalsmässiga och tekniska åtgärder.

11.6 EU:s DORA-förordning (2022/2554):

11.6.1 Artikel 5(2) – styrning av IKT-risker: Kräver att IKT-risker från tredje part, inklusive molntjänster, integreras i den övergripande riskstyrningen.

11.6.2 Artikel 28 – tillsyn över kritiska IKT-leverantörer som tredje part: Kräver att finansiella entiteter övervakar, styr och rapporterar beroenden till molnleverantörer, deras säkerhetsläge och resiliens.

11.7 COBIT 2019:

11.7.1 BAI04 – hantera tillgänglighet och kapacitet: Säkerställer att molntjänster är resilienta, övervakade och uppfyller definierade prestandakriterier.

11.7.2 DSS01 – hantera drift: Stödjer operativ integration, incidenthantering och baskonfigurationer för plattformar i molnmiljö.

11.7.3 DSS05 – hantera säkerhetstjänster: Styr införande av molnspecifika säkerhetskontroller, övervakning och incidentförebyggande åtgärder för digitala tjänster.