					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P27					Dokumenttitel: **Politik for brug af cloudtjenester**							
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 regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Krav til operationel planlægning og styring i cloudmiljøer.
ISO/IEC 27002:2022	Kontroller 5.23–5.25	Krav til brug af cloudtjenester, politik og sikkerhed i cloudtjenester.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Brug af eksterne systemer, kontraktlige og tekniske krav, kryptografiske beskyttelser og beskyttelse af forsyningskæden.
EU GDPR	Artikel 28, 32, kapitel V	Krav til cloududbydere som databehandlere, behandlingssikkerhed og dataoverførsler.
EU NIS2	Artikel 21(2)(f, i)	Krav til tredjepartsrisici og forsyningskæden.
EU DORA	Artikel 5(2), 28	Tilsyn med IKT og tredjeparter (cloud) for finansielle enheder.
COBIT 2019	BAI04, DSS01, DSS05	Tilgængelighed i cloudtjenester samt drifts- og sikkerhedsstyring.

1. Formål

1.1 Denne politik fastsætter organisationens obligatoriske krav til sikker, compliant og ansvarlig brug af cloudtjenester på tværs af leveringsmodellerne Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) og Software-as-a-Service (SaaS).

1.2 Politikken har til formål at sikre, at cloudtjenester tages i brug og styres på en måde, der beskytter fortrolighed, integritet og tilgængelighed (CIA) for informationsaktiver, samtidig med at regulatoriske, juridiske og kontraktlige forpligtelser opfyldes.

1.3 Den fastlægger kontroller til styring af cloudrisici, beskyttelse af data, overvågning af udbyderes efterlevelse og eliminering af uautoriseret brug. Den understøtter også forretningsinnovation gennem cloudplatforme ved at afbalancere sikkerhed, driftsstabilitet og omkostningseffektivitet.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, kontrahenter, tredjepartsleverandører og eksterne konsulenter, som på vegne af organisationen tildeler adgang til, konfigurerer, tilgår, administrerer eller anvender cloudtjenester.

2.2 Den gælder for alle miljøer, hvor organisationens data eller arbejdsbelastninger behandles, herunder:

2.2.1 Offentlige, private, hybride og fællesskabsbaserede cloudimplementeringer

2.2.2 Alle cloudtjenestemodeller (IaaS, PaaS, SaaS)

2.2.3 Multi-cloud- og fødererede arkitekturer

2.2.4 Brug af shadow IT eller personlige cloudkonti til forretningsformål

2.3 Den omfatter alle dataklassificeringer og gælder både for interne systemer og leverandørhostede platforme, hvor organisationsejede eller regulerede data lagres eller behandles.

3. Mål

3.1 At sikre sikker og ensartet brug af cloudteknologier gennem klart definerede retningslinjer for anvendelse, sikkerhedsbaselines og styringsroller.

3.2 At minimere driftsmæssige og regulatoriske risici forbundet med cloud computing, herunder uautoriseret adgang, brud på persondatasikkerheden, fejlkonfiguration, manglende efterlevelse og driftsafbrydelser.

3.3 At håndhæve krav til sikkerhed og databeskyttelse for alle cloudleverandører og verificere efterlevelse gennem kontraktlige klausuler, vurderinger og revisionsrettigheder.

3.4 At muliggøre skalerbar og robust anvendelse af cloudtjenester uden at kompromittere risikobilledet, juridiske krav eller forretningskontinuiteten.

3.5 At tilpasse styring og brug af cloudtjenester til organisationens ISMS, juridiske forpligtelser (f.eks. GDPR, DORA), sektorspecifikke retningslinjer og brancheanerkendt god praksis (f.eks. NIST, COBIT).

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender politikken for brug af cloudtjenester og den strategiske roadmap for anvendelse af cloudtjenester.

4.1.2 Gennemgår og godkender undtagelser med høj risiko fra standardkravene til styring af cloudtjenester.

4.1.3 Sikrer, at cloudinitiativer modtager tilstrækkelig finansiering, styring og integration med organisationens rammer for risikostyring.

4.2 Chief Information Security Officer (CISO)

4.2.1 Ejer denne politik og organisationens Cloud Services Register.

4.2.2 Godkender onboarding af nye cloududbydere på baggrund af due diligence og risikovurdering.

4.2.3 Gennemgår dokumentation for udbyderes efterlevelse og validerer sikkerhedsmæssig overensstemmelse.

[... 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 Denne politik skal gennemgås mindst én gang årligt og opdateres efter behov for at sikre fortsat overensstemmelse med:

9.1.1 udviklende juridiske og regulatoriske krav (f.eks. GDPR, NIS2, DORA)

9.1.2 ændringer i standarderne ISO/IEC 27001 eller ISO/IEC 27002

9.1.3 opdateringer af organisationens cloudarkitektur, trusselslandskab eller serviceportefølje

9.1.4 hændelsesundersøgelser, revisionsresultater eller erfaringer fra driftsmæssig anvendelse

9.2 CISO er ansvarlig for at igangsætte gennemgangen og samle relevante interessenter, herunder:

9.2.1 Cloud Security Architect

9.2.2 jura- og complianceteamet

9.2.3 indkøbs- og leverandøransvarlige

9.2.4 serviceejere og IT-drift

9.3 Alle opdateringer skal være:

9.3.1 versionsstyrede og daterede

9.3.2 godkendt af direktionen

9.3.3 kommunikeret til berørte parter, herunder medarbejdere, kontrahenter og tredjeparter

9.3.4 arkiveret i overensstemmelse med interne politikker for dokumentation

9.4 Midlertidige gennemgange kan udløses af:

9.4.1 nye engagementer med CSP'er eller større migreringer

9.4.2 nye trusler mod cloudinfrastruktur

9.4.3 væsentlige ændringer i kontraktlige, juridiske eller sektorspecifikke forpligtelser

10. Relaterede politikker og sammenhænge

10.1 Denne politik er tæt forbundet med og afhængig af følgende interne politikker:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger de overordnede principper for sikker drift af systemer og tjenester, som denne politik håndhæver i cloudkonteksten.

10.1.2 P5 – Politik for ændringsstyring: Alle ændringer i cloudkonfigurationer skal følge procedurerne for ændringsstyring fastlagt i P5.

10.1.3 P13 – Politik for dataklassificering og mærkning: Fastlægger, hvordan data vurderes før overførsel til cloudmiljøer, og hvordan kontroller som kryptering og dataresidens anvendes.

10.1.4 P18 – Politik for kryptografiske kontroller: Angiver standarder for kryptering, nøglestyring og brug af kryptografiske algoritmer, som anvendes direkte i konfigurationen af cloudtjenester.

10.1.5 P22 – Lognings- og overvågningspolitik: Specificerer krav til indsamling, opbevaring og analyse af logfiler, som skal håndhæves i cloudmiljøer.

10.1.6 P30 – Politik for hændelseshåndtering: Definerer procedurer for eskalering, inddæmning og afhjælpning ved cloudrelaterede sikkerhedshændelser.

10.1.7 P33 – Politik for revisionsberedskab og overvågning af efterlevelse: Understøtter revisionsberedskab og løbende sikkerhed for, at cloudkontroller håndhæves og overvåges.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001: Klausul 8.1 – operationel planlægning og styring: Kræver, at organisationer implementerer og styrer de processer, der er nødvendige for at opfylde kravene til informationssikkerhed, herunder processer, der involverer cloudmiljøer.

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

11.2.1 Bilag A, kontrol 5.23 – brug af cloudtjenester: Kræver risikobaseret vurdering, formel godkendelse og dokumentation af brugen af cloudtjenester.

11.2.2 Bilag A, kontrol 5.24 – politik for brug af cloudtjenester: Kræver etablering og håndhævelse af formelle politikker for brug af cloudtjenester, tilpasset organisationens behov og risici.

11.2.3 Bilag A, kontrol 5.25 – sikkerhed i cloudtjenester: Kræver integration af sikkerhed, kontraktlige beskyttelser og overvågning af cloudhostede arbejdsbelastninger og data.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – brug af eksterne systemer: Kræver definerede regler og betingelser for adgang til organisationens ressourcer fra eksterne eller cloudbaserede systemer.

11.3.2 SA-9(5) – eksterne informationssystemtjenester: Håndhæver kontraktlige sikkerhedskrav, tilsyn og løbende overvågning af tredjeparts cloudsystemer.

11.3.3 SC-12 til SC-28 – kryptografiske beskyttelser, beskyttelse af systemgrænser og transmissionsintegritet: Understøtter krav til kryptering, identitet og adgang for cloudbaserede tjenester og data under overførsel.

11.3.4 SR-5 – beskyttelse af forsyningskæden: Understøtter vurdering og kontraktuel kontrol af CSP'er, der indgår i leveringen af tjenester.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 28 – forpligtelser for databehandlere: Kræver formelle kontrakter med cloududbydere for at sikre sikkerhed, fortrolighed og revisionssporbarhed ved behandling af personoplysninger.

11.4.2 Artikel 32 – behandlingssikkerhed: Understøtter anvendelsen af kryptering, adgangskontroller, logning og andre sikkerhedsforanstaltninger i cloudmiljøer.

11.4.3 Kapitel V – internationale dataoverførsler: Kræver lovlig overførsel af data uden for EU/EØS ved brug af sikkerhedsforanstaltninger som SCC'er eller tilstrækkelighedsafgørelser.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 21(2)(f, i): Kræver, at enheder styrer risici fra tredjeparts cloududbydere og sikrer den digitale forsyningskædes integritet gennem kontraktlige og tekniske foranstaltninger.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5(2) – styring af IKT-risici: Kræver integration af IKT-tredjepartsrisici, herunder cloudtjenester, i den samlede risikostyring.

11.6.2 Artikel 28 – tilsyn med kritiske IKT-tredjepartsudbydere: Kræver, at finansielle enheder overvåger, kontrollerer og rapporterer om afhængigheder af cloududbydere, sikkerhedstilstand og robusthed.

11.7 COBIT 2019:

11.7.1 BAI04 – styring af tilgængelighed og kapacitet: Sikrer, at cloudtjenester er robuste, overvåges og opfylder definerede performancekriterier.

11.7.2 DSS01 – styring af drift: Understøtter driftsmæssig integration, hændelseshåndtering og baselinekonfigurationer på tværs af cloudhostede platforme.

11.7.3 DSS05 – styring af sikkerhedstjenester: Angiver implementering af cloudspecifikke sikkerhedskontroller, overvågning og forebyggelse af hændelser på tværs af digitale tjenester.