| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Indsæt navnet på den registrerede juridiske enhed her | | | | | | | |
| Dokumentnummer:<br>P27S | | | | | Dokumenttitel:<br>**Politik for brug af cloudtjenester** | | | | | | | |
| Version:<br>1.0 | | Ikrafttrædelsesdato:<br>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 | Kapitel 8 | |
| ISO/IEC 27002:2022 | Kontroller 5.23–5.25 | |
| NIST SP 800-53 Rev. 5 | AC-20, SC-12, SC-13, SR-5 | |
| EU GDPR | Artikel 28, 32 og kapitel V | |
| EU NIS2 | Artikel 21(2)(f), (i) | |
| EU DORA | Artikel 5(2), 28 | |
| COBIT 2019 | DSS01, DSS05, BAI04 | |

**1. Formål**

1.1 Denne politik fastlægger, hvordan cloudtjenester må anvendes sikkert i organisationen. Den sikrer, at data, der behandles eller opbevares i cloudtjenester, beskyttes, at adgang styres, og at risici håndteres forsvarligt.

1.2 Den hjælper SMV'er med at opfylde juridiske forpligtelser og kunders forventninger til beskyttelse af følsomme oplysninger, forebyggelse af datalæk og effektiv håndtering af cloudrelaterede risici uden krav om infrastruktur i enterprise-skala.

1.3 Denne politik understøtter ISO/IEC 27001-certificering, efterlevelse af GDPR og sikkerhed i forsyningskæden gennem konsekvent styring af alle tredjeparts-cloudtjenester.

**2. Omfang**

**2.1 Denne politik gælder for:**

2.1.1 Enhver cloudbaseret tjeneste, der anvendes til at opbevare, behandle eller overføre virksomhedens data

2.1.2 Alle medarbejdere, kontrahenter eller tjenesteudbydere, der anvender cloudværktøjer på vegne af organisationen

2.1.3 Gratis og betalte cloudløsninger, herunder e-mail-platforme, dokumentdeling, SaaS-værktøjer, backupplatforme, videokonferencer og kundeplatforme

2.1.4 Enhver enhed (stationære computere, mobile enheder, tablets), der tilgår virksomhedens oplysninger via cloudapplikationer

**2.2 Dette omfatter blandt andet:**

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Cloudbaserede værktøjer til backup og katastrofeberedskab

2.2.5 Delte mapper eller applikationer, der anvendes til fakturering, projektstyring eller kundekommunikation

**3. Mål**

3.1 Forebygge uautoriseret brug eller højrisikobrug af ikke-godkendte cloudtjenester.

3.2 Sikre, at følsomme eller regulerede data, der opbevares i cloudtjenester, beskyttes ved hjælp af passende tekniske og organisatoriske kontroller.

3.3 Fastlægge tydelige roller for godkendelse, konfiguration, overvågning og udfasning af cloudtjenester.

3.4 Styre dataflows og håndhæve forpligtelser vedrørende opbevaring, sletning og databeskyttelse for oplysninger, der opbevares i cloudtjenester.

3.5 Reducere afhængigheden af personlige konti eller ikke-sporede værktøjer ved at kræve godkendelse af alle cloudsystemer, der anvendes til forretningsformål.

3.6 Efterleve krav i ISO/IEC 27001:2022, GDPR, NIS2 og DORA ved håndtering af eksterne cloudafhængigheder.

## 4. Roller og ansvar

### 4.1 Direktør (GM)

4.1.1 Godkender brugen af alle nye cloudtjenester

4.1.2 Gennemgår risici relateret til cloudleverandører og tjenestetyper

4.1.3 Håndhæver politikken og fører tilsyn med beslutninger om undtagelser

### 4.2 Ekstern it-leverandør eller teknisk support

4.2.1 Evaluerer og implementerer sikker konfiguration af cloudtjenester

4.2.2 Etablerer konti, adgangskontroller og backup-løsninger

4.2.3 Overvåger efterlevelse af krav til adgangskoder, MFA og sikkerhedsindstillinger

[ ... 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 af direktøren i koordinering med den eksterne it-leverandør.

### 9.2 En formel gennemgang skal også finde sted:

9.2.1 Efter en cloudrelateret sikkerhedshændelse (f.eks. brud, datatab)

9.2.2 Når en ny væsentlig cloudplatform indføres

9.2.3 Hvis juridiske eller regulatoriske krav ændres (f.eks. opdateringer til GDPR, NIS2 eller DORA)

9.2.4 Hvis overvågningsaktiviteter afdækker misbrug eller nye risici

### 9.3 GM skal sikre:

9.3.1 At registeret over cloudtjenester opdateres med nye eller udfasede tjenester

9.3.2 At juridiske krav og krav til databeskyttelse fortsat opfyldes

9.3.3 At alle ændringer kommunikeres til relevante brugere og interessenter

9.4 Arkiverede versioner skal opbevares sikkert, og tidligere versioner af politikken skal håndteres i overensstemmelse med organisationens P14S – Politik for dataopbevaring og bortskaffelse.

## 10. Relaterede politikker og sammenhænge

### 10.1 Denne politik skal anvendes i sammenhæng med følgende informationssikkerhedspolitikker tilpasset SMV'er:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Definerer ansvarlighed for godkendelse af cloudtjenester og styring af relationer til udbydere.

10.1.2 P4S – Politik for adgangskontrol: Understøtter sikker login, sessionsstyring og praksis for tilbagekaldelse, som kræves for cloudplatforme.

10.1.3 P14S – Politik for dataopbevaring og bortskaffelse: Regulerer, hvordan cloudbaserede data sikkerhedskopieres, opbevares og slettes i overensstemmelse med juridiske forpligtelser.

10.1.4 P17S – Politik for databeskyttelse og privatliv: Sikrer, at personoplysninger, der opbevares i cloudtjenester, håndteres i overensstemmelse med GDPR-principperne.

10.1.5 P30S – Politik for hændelseshåndtering: Indeholder strukturerede procedurer for håndtering af sikkerhedshændelser i cloudmiljøer, herunder indsamling af digitale beviser og ekstern underretning.

10.2 Samlet set sikrer disse politikker, at brugen af cloudtjenester er sikker, sker i overensstemmelse med kravene og understøtter operationel robusthed.

## 11. Referencestandarder og rammeværker

### 11.1 ISO/IEC 27001

11.1.1 Kapitel 8.1 – Kræver, at organisationer implementerer operationelle kontroller for datahåndtering, herunder kontroller relateret til cloudbaserede systemer.

### 11.2 ISO/IEC 27002

11.2.1 Kontrol 5.23 – Kræver styring af brugen af cloudtjenester og tredjeparts-SaaS-værktøjer.

11.2.2 Kontrol 5.24 – Kræver en defineret politik for brug af cloudtjenester, der er tilpasset risici og regulatoriske krav.

11.2.3 Kontrol 5.25 – Kræver, at organisationer sikrer, at sikkerhedskontroller i cloudmiljøer opfylder organisationens behov.

### 11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Kræver formelle politikker for brug af eksterne systemer såsom cloudtjenester.

11.3.2 SC-12, SC-13 – Omhandler kryptering af data under overførsel og data i hvile i cloudmiljøer.

11.3.3 SR-5 – Omfatter kontroller for cloud- og tredjepartsrisici i forsyningskæden.

### 11.4 EU GDPR (2016/679)

11.4.1 Artikel 28 – Kræver, at cloududbydere, der fungerer som databehandlere, er underlagt bindende kontraktlige forpligtelser.

11.4.2 Artikel 32 – Kræver tekniske og organisatoriske kontroller for cloudbaseret databehandling.

11.4.3 Kapitel V – Forbyder uautoriserede internationale overførsler af personoplysninger, der opbevares i cloudtjenester.

### 11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(f), (i) – Kræver, at væsentlige og vigtige enheder implementerer passende politikker for sikkerhed i cloudtjenester og kontrol med forsyningskæden.

### 11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2) – Kræver, at finansielle SMV'er integrerer cloudsikkerhed i deres styringsrammer for IKT-risikostyring.

11.6.2 Artikel 28 – Fastlægger regler for tilsyn med kritiske tredjeparts-IKT-tjenesteudbydere, herunder cloudleverandører.

### 11.7 COBIT 2019

11.7.1 DSS01 – "Manage Operations" omhandler den operationelle integritet af cloudtjenester.

11.7.2 DSS05 – "Manage Security Services" omfatter cloudspecifik beskyttelse og overvågning.

11.7.3 BAI04 – "Manage Availability and Capacity" sikrer forretningskontinuitet og ydeevne i cloudmiljøer.