| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ange namnet på den registrerade juridiska personen här | | | | | | | |
| Dokumentnummer:<br>P27S | | | | | Dokumenttitel:<br>**Policy för användning av molntjänster** | | | | | | | |
| Version:<br>1.0 | | Ikraftträdandedatum:<br>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 | |
| ISO/IEC 27002:2022 | Kontroll 5.23–5.25 | |
| NIST SP 800-53 Rev. 5 | AC-20, SC-12, SC-13, SR-5 | |
| EU:s GDPR | Artikel 28, 32 och kapitel V | |
| EU:s NIS2-direktiv | Artikel 21.2 f, i | |
| EU:s DORA-förordning | Artikel 5.2, 28 | |
| COBIT 2019 | DSS01, DSS05, BAI04 | |

**1. Syfte**

1.1 Denna policy fastställer hur molntjänster får användas på ett säkert sätt inom organisationen. Den säkerställer att data som behandlas eller lagras i molnet skyddas, att åtkomst styrs och att risker hanteras på ett ansvarsfullt sätt.

1.2 Denna policy hjälper SME-företag att uppfylla rättsliga skyldigheter och kundkrav avseende skydd av känslig information, förebyggande av dataläckage samt effektiv hantering av molnrelaterade risker utan krav på infrastruktur i företagsklass.

1.3 Denna policy stödjer certifiering enligt ISO/IEC 27001, efterlevnad av EU:s GDPR och säkerställande av leveranskedjan genom en konsekvent styrning av samtliga molntjänster från tredje part.

**2. Omfattning**

**2.1 Denna policy gäller för:**

2.1.1 Alla molnbaserade tjänster som används för att lagra, behandla eller överföra företagets data

2.1.2 All personal, entreprenörer och tjänsteleverantörer som använder molntjänster på uppdrag av organisationen

2.1.3 Kostnadsfria och betalda molnlösningar, inklusive e-postplattformar, dokumentdelning, SaaS-tjänster, plattformar för säkerhetskopiering, videokonferenser och kundplattformar

2.1.4 Alla enheter (stationära datorer, mobiler, surfplattor) som används för åtkomst till företagsinformation via molnapplikationer

**2.2 Detta omfattar bland annat:**

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 Molnbaserade verktyg för säkerhetskopiering och katastrofåterställning

2.2.5 Delade mappar eller applikationer som används för fakturering, projektledning eller kundkommunikation

**3. Mål**

3.1 Förhindra obehörig användning eller användning med hög risk av icke godkända molntjänster.

3.2 Säkerställa att känsliga eller reglerade data som lagras i molnet skyddas genom lämpliga tekniska och administrativa kontroller.

3.3 Fastställa tydliga roller för godkännande, konfigurering, övervakning och avveckling av molntjänster.

3.4 Styra dataflöden och säkerställa krav avseende bevarande, radering och dataskydd för information som lagras i molnet.

3.5 Minska beroendet av personliga konton eller ospårade verktyg genom att kräva godkännande av alla molnsystem som används för verksamhetsändamål.

3.6 Uppfylla krav enligt ISO/IEC 27001:2022, EU:s GDPR, EU:s NIS2-direktiv och EU:s DORA-förordning för hantering av externa molnberoenden.

**4. Roller och ansvar**

**4.1 Verkställande direktör (VD)**

4.1.1 Godkänner användning av alla nya molntjänster

4.1.2 Granskar risker kopplade till molnleverantörer och tjänstetyper

4.1.3 Säkerställer efterlevnad av denna policy och utövar tillsyn över beslut om undantag

**4.2 IT-supportleverantör eller teknisk supportfunktion**

4.2.1 Utvärderar och inför säker konfiguration för molntjänster

4.2.2 Upprättar konton, åtkomstkontroller och säkerhetskopiering

4.2.3 Övervakar efterlevnad av krav på lösenord, flerfaktorsautentisering (MFA) och säkerhetsinställningar

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

**9. Krav på granskning och uppdatering**

9.1 Denna policy ska granskas minst årligen av verkställande direktör i samordning med IT-supportleverantören.

**9.2 En formell granskning ska även genomföras:**

9.2.1 Efter en molnrelaterad säkerhetsincident (t.ex. intrång, dataförlust)

9.2.2 När en ny större molnplattform införs

9.2.3 Om rättsliga eller regulatoriska krav ändras (t.ex. uppdateringar av EU:s GDPR, EU:s NIS2-direktiv eller EU:s DORA-förordning)

9.2.4 Om övervakningsaktiviteter visar på felaktig användning eller nya risker

**9.3 Verkställande direktör ska säkerställa:**

9.3.1 Att registret över molntjänster uppdateras med nya eller avvecklade tjänster

9.3.2 Att rättsliga krav och krav på dataskydd fortsatt uppfylls

9.3.3 Att alla ändringar kommuniceras till relevanta användare och intressenter

9.4 Arkiverade versioner ska lagras säkert, och äldre versioner av policyn ska hanteras enligt organisationens P14S – Policy för databevarande och bortskaffande.

**10. Relaterade policyer och kopplingar**

**10.1 Denna policy ska tillämpas tillsammans med följande SME-anpassade informationssäkerhetspolicyer:**

10.1.1 P2S – Policy för styrningsroller och ansvar: Definierar ansvar för godkännande av molntjänster och hantering av leverantörsrelationer.

10.1.2 P4S – Policy för åtkomstkontroll: Stödjer säker inloggning, sessionshantering och rutiner för avveckling av behörigheter som krävs för molnplattformar.

10.1.3 P14S – Policy för databevarande och bortskaffande: Reglerar hur molnbaserade data säkerhetskopieras, bevaras och raderas i enlighet med rättsliga skyldigheter.

10.1.4 P17S – Policy för dataskydd och integritet: Säkerställer att personuppgifter som lagras i molntjänster hanteras enligt principerna i EU:s GDPR.

10.1.5 P30S – Policy för incidenthantering: Tillhandahåller strukturerade rutiner för hantering av säkerhetsincidenter i molnmiljöer, inklusive insamling av bevismaterial och extern avisering.

10.2 Tillsammans säkerställer dessa policyer att användningen av molntjänster är säker, regelefterlevande och operativt robust.

## 11. Referensstandarder och ramverk

### 11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver att organisationer inför operativa kontroller för datahantering, inklusive kontroller som avser molnbaserade system.

### 11.2 ISO/IEC 27002

11.2.1 Kontroll 5.23 – Kräver styrning av användning av molntjänster och SaaS-tjänster från tredje part.

11.2.2 Kontroll 5.24 – Kräver en definierad policy för användning av molntjänster i linje med risker och regulatoriska krav.

11.2.3 Kontroll 5.25 – Kräver att organisationer säkerställer att säkerhetskontroller i molnmiljö uppfyller organisationens behov.

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

11.3.1 AC-20 – Kräver formella användningspolicyer för externa system såsom molntjänster.

11.3.2 SC-12, SC-13 – Omfattar kryptering av data under överföring och data i vila i molnmiljöer.

11.3.3 SR-5 – Omfattar riskkontroller för molntjänster och tredje part i leveranskedjan.

### 11.4 EU:s GDPR (2016/679)

11.4.1 Artikel 28 – Kräver att molnleverantörer som agerar som personuppgiftsbiträden följer bindande avtalsförpliktelser.

11.4.2 Artikel 32 – Kräver tekniska och organisatoriska kontroller för molnbaserad behandling av personuppgifter.

11.4.3 Kapitel V – Förbjuder obehöriga internationella överföringar av personuppgifter som lagras i molnet.

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

11.5.1 Artikel 21.2 f, i – Kräver att väsentliga och viktiga entiteter inför lämpliga policyer för säkerhet i molntjänster och kontroll av leveranskedjan.

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

11.6.1 Artikel 5.2 – Kräver att finansiella SME-företag integrerar molnsäkerhet i sina ramverk för hantering av IKT-risker.

11.6.2 Artikel 28 – Fastställer regler för tillsyn över kritiska tredjepartsleverantörer av IKT-tjänster, inklusive molnleverantörer.

### 11.7 COBIT 2019

11.7.1 DSS01 – ”Manage Operations” behandlar den operativa integriteten i molntjänster.

11.7.2 DSS05 – ”Manage Security Services” omfattar molnspecifika skyddsåtgärder och övervakning.

11.7.3 BAI04 – ”Manage Availability and Capacity” säkerställer verksamhetskontinuitet och prestanda i molnmiljöer.