Riktlinje för molntjänster

Kommunalförbundet ITSAM och dess medlemskommuner

Fastställd: 20161227
Ersätter: 20160821

1.0 Syfte

Syftet med denna riktlinje är att övergripande definiera regelverket och kraven avseende införskaffande, användningen och avvecklingen av externa och interna molnbaserade tjänster utifrån gällande säkerhetsnivåer avseende tillgänglighet, sekretess, riktighet, integritet och spårbarhet.

Med molntjänst menas tjänster i form av infrastruktur, funktion eller applikation som levereras eller erbjuds som tjänst över internet eller intranät via webbaserade gränssnitt. Det som utmärker en molntjänst är att hårdvaran kan vara skild från kommunalförbundet och att ansvaret för drift i dessa fall ligger på extern leverantör. Molntjänster levereras från datacenters som kan vara placerade i egen organisation eller externt var som helst i världen. I och med detta är det ett krav att före införskaffandet av molntjänster ta fram risk- och sårbarhetsanalyser och bedöma bl. a. vilken typ av information som kommer att hanteras av molntjänsten. Analyserna ska, utifrån interna regelverk samt lagar och förordningar i det land informationen lagras och bearbetas och att detta inte strider mot nationella lagar och förordningar, ge en kravbild på införskaffande och användning av molntjänsten.

2.0 Omfattning

Denna riktlinje omfattar informationsägare, systemägare, systemförvaltare och driftansvariga inom kommunalförbundet samt externa leverantörer av molntjänster. Med systemägare i denna riktlinje avses den verksamhet eller organisation som är informationsägare till den information tjänsten, interna eller externa, bearbetar. Kommunalförbundets systemägare är den kravställande parten vid kontraktering av interna eller externa tjänster.

Riktlinjen omfattar alla typer av tjänster, både kommunalförbundets egna tjänster och tjänster från externa leverantörer i de fall interna molntjänster implementeras och publiceras via internet. Det kan dels vara från kommersiell part där man köper tillgång till applikationer, funktion, lagring eller infrastruktur såsom serverkapacitet, och dels från andra samarbetsorganisationer där man samverkar kring gemensamma system.

Riktlinjen omfattar följande tjänstetyper inom kommunalförbundet:

- **Applikation**
- **Funktion**
- **Infrastruktur**

3.0 Molntyper

- **Privata moln:** Ansvaret för drift av applikation, funktion, lagring och infrastruktur ligger inom den egna organisationen. Information bearbetas och lagras internt.
- **Publika moln:** Applikationer, funktioner, lagring och infrastruktur finns tillgängligt för alla.
- **Hybridmoln:** En process där informationen bearbetas både i privata och publika moln.
- **Partnermoln:** Samverkansparter skapar relationer mellan organisationerna för att nyttja varandras lagring, funktion eller infrastruktur.

4.0 Tjänstetyper

4.1 Software as a Service, SaaS
SaaS är benämningen på tjänstetyp där applikationer exekveras hos leverantören av moln. Denna presenteras över internet eller intranät och via webbaserade gränssnitt. Leverantören av SaaS ansvarar för uppgraderingar och konfiguration av applikationerna. Annan benämning är AaaS *Application as a Service*.

4.2 Infrastructure as a Service, IaaS
IaaS är benämningen på tjänstetyp där serverkapacitet såsom CPU, RAM, lagring, kommunikation etc. finns externt hos leverantören av tjänsten. Leverantör ansvarar för drift av serverkapaciteten och kan dynamiskt minska eller öka denna utifrån användarens behov.

4.3 Platform as a Service, PaaS
PaaS är benämningen på tjänstetyp där leverantören av molntjänsten erbjuder en extern utvecklingsplattform och där användaren kan utveckla och testköra sin mjukvara. Leverantören ansvarar för drift och underhåll av bakomliggande mjukvara för denna plattform.

Interna tjänstetyper kan förekomma men ingår då i någon av ovanstående grundtyper. Inom kommunalförbundet finns bl. a implementerat plattform för virtuella skrivbord och som benämns DaaS, *Desktop as a Service* men som är av grundtypen IaaS. Samtliga inom kommunalförbundet förekommande molntjänster inklusive relationer ska finnas förtecknade enligt *informationssäkerhetsinstruktion Kontinuitet och Drift*.

5.0 Definitioner

5.1 Tjänstemäklare, CB
CB som står för *Cloud Broker* är part som skapar och upprätthåller relationer med flera molntjänsteleverantörer. CB fungerar som en länk mellan leverantörer av molntjänster och kommunalförbundet. Exempel på CB är där federationer skapas mellan CB och kommunalförbundet och där identifiering och autentisering sker en gång oavsett mängden bakomliggande leverantörer och de molntjänster som används.

5.2 Tjänsteleverantör, CSP
CSP som står för *Cloud Service Provider* är en organisation som tillhandahåller molnbaserade plattformar, infrastruktur, applikationer, säkerhet eller lagringstjänster för egen eller annan organisation. ITSAM eller extern kontrakterad organisation kan vara tjänsteleverantör.

5.3 Arkitektur, CSA
CSA som står för *Cloud Service Architecture* är strukturen och uppbyggnaden av system som bildar den arkitektur där applikationer och funktioner fungerar som tjänster på internet eller på kommunalförbundets intranät.

5.4 Tjänsteklassificering
Inom kommunalförbundet ska information och informationsbärande system vara förtecknade och klassificerade utifrån interna och externa krav. Molnbaserat informationsbärande system som

hanterar den egna organisationens information ska klassificeras såsom för traditionella interna verksamhetssystem.

Tillämpade nivåer är:

1 = Oklassificerad: Publik information. Tjänst som bearbetar information vars röjande orsakar försumbar skada för person, kommunalförbundet och dess verksamheter.
2 = Intern: Interna tillgångar. Tjänst som bearbetar information vars röjande kan orsaka måttlig skada för person, kommunalförbundet och dess verksamheter.
3 = Begränsad: Tillgång ges till definierade användare, roller eller användargrupper. Tjänst som bearbetar information vars röjande kan orsaka betydande skada för person, kommunalförbundet och dess verksamheter.
4 = Sekretesskyddad: Konfidentiell information begränsad till få behöriga personer. Tjänst som bearbetar information vars röjande kan orsaka allvarlig skada för person, kommunalförbundet och dess verksamheter.

5.5 Federation

Med federation menas att på teknisk väg skapa och upprätthålla ett förtroende mellan två skilda organisationer för att samverka och nyttja varandras tjänster och funktioner. Information såsom identiteter, lösenord och data kan strömma mellan organisationerna via publika nät på ett säkert sätt.
Gemensamma regelverk bestäms för att i federationen nå basnivåerna avseende tillgänglighet, sekretess, riktighet, integritet, och spårbarhet.

5.6 Service Level Agreement, SLA

Tillgänglighetsgraden till applikationer, funktioner och övriga tjänster är av betydelse och styrs bl. a klassificering av den information dessa bearbetar. Oavsett molntyper, ska SLA-nivåer finnas och som ska täcka upp det eventuella tillgänglighetsbehovet som finns eller uppstår.
SLA beskriver den garanterade tiden system ska vara tillgängliga samt åtgärdstider vid fel och maximal tid då system inte är tillgängliga.

6.0 Riktlinje

6.1 Hantering av molnbaserade tjänster

Att flytta datatillgångar in i molnet kan kräva omläggning av bl. a. service och support. Roller och ansvar förändras när en organisation använder molntjänster. Av denna anledning måste organisationer tydligt definiera roller för att hantera leverantörsrelationer avseende service och support.

6.1.1 Utbildning

Inom kommunalförbundet ska det finnas utbildad personal inom molnarkitektur på ett tekniskt och administrativt plan.

6.1.2 Roller och ansvar

Inom kommunalförbundet ska det finnas definierade och dokumenterade roller och ansvarsområden såsom kravställning, upphandling, förändringshantering, säkerhet etc. för personal som ansvarar för att hantera molntjänster. Dessa roller och ansvarsområden definieras i

Informationssäkerhetsinstruktion Förvaltning
Inom kommunalförbundet bör finnas eller upprättas RACI-matriser eller liknande för varje enskilt system och för varje enskild tjänst.

6.2 Säkerhet i molnet

Alla verksamheter inom kommunalförbundet är bundna till denna riktlinje. Kommunerna inom kommunalförbundet är informationsägare till verksamhetssystem dessa äger och förvaltar på en administrativ och operativ nivå. Lokala regelverk kan förekomma men ska då harmoniera med denna riktlinje. Kommunicering av regelverk och riktlinjer till anställda i verksamheten ansvarar verksamheternas ledning för med stöd av kommunalförbundet.

Riktlinjen ska revideras kontinuerligt eller om förändringar sker för att säkerställa dess fortsatta riktighet och lämplighet. Exempel på förändringar är arkitekturändringar, ändring av tjänst, större serviceuppgraderingar eller förändring av tjänsteleverantör.

Verksamheten skall se till att leverantör av molntjänster har passerat alla nödvändiga säkerhetskrav som bedöms av IT- och informationssäkerhetsansvariga och personuppgiftsansvarig utifrån interna och externa regelverk inom kommunalförbundet. Krav på att kontinuerliga risk- och sårbarhetsanalyser ska utföras och där detta ska framgå. Verksamheter inom kommunalförbundet får inte teckna avtal med en tjänsteleverantör utan att alla krav är uppfyllda enligt framtagen checklista, se *Checklista molntjänstleverantör*.

6.2.1 Uppdatering och uppgradering

Systemägaren för respektive molntjänst ska komma överens med tjänsteleverantör om lämpliga uppdaterings- och uppgraderingsintervall för sådant som kan påverka säkerhetsnivåerna avseende tillgänglighet, sekretess, integritet och spårbarhet samt sådant som kan påverka kravbilden utifrån ett juridiskt perspektiv.

6.2.2 Riskhantering

Systemägare och driftansvariga inom kommunalförbundet ska begära och bedöma detaljerad information om hur tjänsteleverantör säkerställer och tillämpar riskhantering före kontraktering av tjänsteleverantör. Optimering av kommunalförbundets egna processer gällande riskhantering med tillhörande verktyg ska genomföras för att effektivisera och smidiggöra eventuella distributioner i molnet.

Kommunalförbundet ska kunna begära och validera, före och efter kontraktering, leverantörens metodik avseende riskhantering och att tillämpad metodik ligger inom ramen för nationell och internationell standard som beskrivs i ISO27000, COBIT etc.

6.2.3 Förändringshantering

Inom kommunalförbundet ska finnas funktion för förändringshantering. Denna ska löpande meddelas om förändringar av tjänster och som påverkar säkerhetsnivåerna avseende tillgänglighet, sekretess, integritet och spårbarhet samt sådant som kan påverka kravbilden utifrån ett juridiskt perspektiv.
Leverantörens process avseende förändringshantering ska vara känd och tydliga kontaktvägar ska finnas mellan kommunalförbundet och tjänsteleverantören. Metodik och ramverk avseende

förändringshantering ska harmoniera med metodik och ramverk såsom ITIL etc. tillämpad inom kommunalförbundet.

6.3 Virtualisering

I molnets infrastruktur är de flesta logiska avgränsningarna inte av fysisk karaktär såsom separata servrar etc. Avgränsningen avseende segmentering och integritet säkerställs genom att en logisk arkitektur avseende kontroller för system och applikationer utformats. En gemensam mekanism för att tillhandahålla denna avgränsning av data och tjänster är virtualisering.

6.3.1 Systemskydd, härdning

Med systemskydd menas att hantering, konfiguration, åtkomst görs på sådant sätt att risken för incidenter elimineras eller decimeras till en godtagbar nivå.
Checklista för att uppfylla gällande säkerhetsnivåer och för att säkerställa integritet för information och informationsbärande system i en virtuell infrastruktur ska inkludera men inte begränsas till

- inaktivering eller borttagning av alla icke nödvändiga gränssnitt, enheter och tjänster
- konfigurering av nätverksgränssnitt och lagringsutrymmen på ett säkert sätt
- att sätta begränsningar på åtkomst till resurser i den virtuella miljön
- att säkerställa att operativsystem och applikationer som körs i den virtuella miljön härdas
- att validera integriteten vid hanteringen av eventuella kryptonycklar
- härdning av den virtuella miljöns hårdvara

6.3.2 Hantering av virtuella maskiner

Systemägare ska se till att tjänsteleverantör har implementerade kontroller för att garantera att endast behöriga ögonblicksbilder tas, och att dessa ögonblicksbilders nivå avseende klassificering, lagringsplats och kryptering är i nivå med systemets grundklassificering enligt kommunalförbundets standard.

6.3.3 Hypervisor

Skiktet mellan hårdvaran och virtuella maskiner hanterar, fördelar och balanserar hårdvaruresurser till de virtuella enheterna. Systemägare inom kommunalförbundet ska försäkra sig att följande kontroller är tillämpade:

- Att ansvariga inom kommunalförbundet har åtkomst till administrativa åtkomstloggar.
- Att fullständig loggning är påslagen.

6.4 Identitetshantering och logghantering

6.4.1 Federerad identitet

Kommunalförbundet bör följa standarder såsom SAML 2 etc. och använda det vid identifiering och autentisering mot tjänsteleverantör.

6.4.2 Active Directory autentisering

Kommunalförbundet får inte bevilja tillstånd för extern tjänsteleverantör att direkt använda eller ge tillgång till autentisering mot kommunalförbundets huvudkatalog, AD. Identifiering, autentisering och auktorisation ska ske via RADIUS, DIAMETER, TACACS+ eller motsvarande och enligt kommunalförbundets standard.

För interna, privata och organisatoriska moln ska autentisering ske via RADIUS, DIAMETER, TACACS+ eller motsvarande såsom för externa leverantörer.

6.4.3 Flerfaktorsautentisering

Kommunalförbundet eller extern tjänsteleverantör ska ha stöd för flerfaktorautentisering såsom certifikatbaserad token på annan enhet, engångslösenord (OTP) etc. för autentisering mot molntjänst där så krävs.

6.4.4 Identitetshantering

Vid val av extern tjänsteleverantör ska kommunalförbundet ges möjlighet att själv hantera sina egna identiteter såsom skapande och radering av dessa. Kommunalförbundet ska försäkra sig att autentiseringsprocess, åtkomstkontroll, ansvarighet och loggning uppfyller lagstadgade och juridiska krav i de fall den hanterade informationen faller inom ramen för dessa.

6.4.5 Loggning

Systemägaren ska försäkra sig om att loggning är aktiverad för alla typer av händelser som är av betydelse avseende IT- och informationssäkerhet. Bedömning i vilken omfattning loggar ska sparas ska göras i varje enskilt fall då tjänst ska implementeras och göras tillgänglig för användare och beror på tjänstens klassificering.

6.5 Kris- och incidenthantering

Kommunalförbundet ska försäkra sig om att tjänsteleverantörens processer kring incident- och förändringshantering överensstämmer med kommunalförbundets egna standardprocesser utifrån det som anges i ITIL.

6.6 Kontinuitets- och återställningsplan

Driftansvariga inom kommunalförbundet ska ha tillgång till tjänsteleverantörens kontinuitets- och återställningsplaner i de delar som berör kommunalförbundet. Detta för att försäkra sig att dessa harmonieras och överensstämmer med kommunalförbundets övriga planer i de delar som omfattar drift och kontinuitet för de aktuella tjänsterna. Kommunalförbundet ska också

- meddelas hur och när återställning av förlorad data kan ske
- få löpande rapportering kring tester av planerna
- bli försäkrade att ordinarie säkerhetsnivåer beroende på klassificering nås då återställning av system eller data sker
- bli försäkrade att kris- och incidenthanteringen samt funktion för återställning helt ägs och hanteras av den kontrakterade leverantören.

6.7 Avtal och kontrakt

Innan beslut om flytt av en tjänst till tredje part bör en noggrann juridisk analys och utvärdering genomföras.

6.7.1 Sekretessavtal
Informationsägaren, organisation inom kommunalförbundet, ska teckna sekretessavtal med tjänsteleverantör i de fall information som bearbetas av tjänst är sekretesskyddad. Personlig information, PII (Personlig identitetsinformation) samt arbetsmaterial får inte vidareförmedlas till tredje part och där avtal saknas med organisation inom kommunalförbundet.

6.7.2 Informationsägare
Organisation inom kommunalförbundet ska ha exklusiv äganderätt till egen producerad data eller personuppgifter under avtalstiden. Ägandet omfattar kopior av data tillgängliga genom tjänsteleverantör inklusive säkerhetskopior om sådana finns. Det är inte tillåtet att använda informationen för reklam eller för andra ej överenskomna ändamål.

6.7.3 Lagring
Det ska framgå i kontrakt med tjänsteleverantör var information som hanteras av tjänst lagras och vilka geografiska placeringar som är acceptabla utifrån förordningar och lagstiftning samt utifrån interna regelverk.

6.7.4 Legala krav
Kommunalförbundet ska försäkra sig att tjänsteleverantörens sekretesspolicy överensstämmer med tillämpliga lagar i Sverige.

6.7.5 Dataintrång
Kommunalförbundet ska meddelas inom överenskommen tid vid bekräftade dataintrång hos tjänsteleverantör. Tjänsteleverantör står som ansvarig i de fall överenskomna säkerhetsnivåer avseende tillgänglighet, integritet, sekretess inte nås och som drabbar part inom kommunalförbundet.

6.7.6 Avveckling av tjänst
Vid upphörande av tjänst ska tjänsteleverantören eliminera och radera alla spår av data tillhörande kommunalförbundet och som lagrats hos tjänsteleverantören. Kommunalförbundet ansvarar för att, i de fall data ska arkiveras, säkerställa innehållet till arkivfunktion innan upphörandet av tjänsteleverans enligt gällande lagar och regler om bevarande av information.
Data som hanteras av molntjänst och som ska, efter avveckling av tjänst, bevaras eller överföras till annat system ska ha kompatibelt standardiserat format för att säkerställa överföringen, se *Riktlinje gällande anskaffning och avveckling av informationsbärande system.*

7.0 Verkställighet
Olika metoder används för att kontrollera efterlevnaden av denna riktlinje. Detta innebär, men är inte begränsat till, stickprovskontroller, analys och övervakning av åtaganden i form av avtalade SLA-nivåer, uppfyllande av externa och interna regelverk, datatrafik samt löpande behörighetskontroller. Rapportering och revision görs löpande.

Organisation eller användare som bryter mot denna riktlinje kan bli föremål för disciplinära åtgärder såsom spärr av tjänst, fråntagande av behörigheter och i vissa fall polisanmälan.

8.0 Relaterade dokument

0-0-0 Informationssäkerhetspolicy IT_20130926.pdf
2-0-0 Informationssäkerhetsinstruktion Kontinuitet och Drift IT- Infosäk KD 20151111.pdf
Checklista molntjänstleverantör.pdf