STYRDOKUMENT

Riktlinjer för utkontraktering av IT

Beslutad när	2021-02-04 § 16
Beslutad av	Kommunfullmäktige
Diarienummer	KSKF/2020:190
Ersätter	Riktlinje för Eskilstuna kommuns IT-verksamhet KSKF 2017:655
Gäller för	Samtliga nämnder och följande bolag
Gäller fr o m	2021-02-04
Gäller t o m	Tillsvidare
Dokumentansvarig	IT för Eskilstuna kommun
Uppföljning	

Program
Ett program är ett styrande dokument som ska visa en färdriktning genom att innehålla vad som ska uppnås inom ett visst område. Det tar inte ställning till utförande, prioriteringar och metoder. Program ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige eller av berörd nämnd.

Plan
En plan är ett styrande dokument som ska visa en färdriktning genom att innehålla konkreta mål och riktlinjer. Den ska vara tidsbegränsad och beslutas av kommunfullmäktige eller av berörd nämnd.

Policy
En policy är ett styrande dokument som ska visa ett övergripande förhållningssätt och som ska tjäna som vägledning inom ett område, med angivande av övergripande mål och värden som ska eftersträvas. Policys ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige.

Riktlinje
En riktlinje är ett styrande dokument som ska säkerställa ett korrekt agerande och god kvalitet i handläggning och utförande. Riktlinjer ska vara långsiktiga, ej tidsbegränsade och beslutas av kommunfullmäktige eller av berörd nämnd.

Inledning

Denna riktlinje är ett komplement till Eskilstuna kommuns IT-policy och Riktlinjen för anskaffning av IT. Inom denna riktlinje beskrivs vilka principer som gäller vid beslut om utkontraktering av IT-tjänster inom kommunkoncernen.

Bakgrunden till riktlinjen är att kommunkoncernen idag har en rik flora av system som inte kan integreras eller hanteras på ett ändamålsenligt och effektivt sätt, vilket är en förutsättning för digitaliseringsarbetet.

Utkontraktering benämns ofta som outsourcing eller enbart sourcing. I denna riktlinje används begreppet ”sourcing” och avser då alla former av utkontraktering av system, tjänster, kompetens och infrastruktur till extern part utanför kommunkoncernen inklusive molntjänster.

Riktlinjen omfattar alla nämnder och bolag inom koncernen.
Kort beskrivning av själva området och bakgrunden. Mer omfattande beskrivningar ska skrivas i en separat handling som läggs som en bilaga i ärendet.

Riktlinjes syfte

Syftet med denna riktlinje är att säkerställa att all sourcing av IT sker på ett ändamålsenligt och hållbart sätt samt i enlighet med koncernens målarkitekturer och objektsförvaltningsplaner. Riktlinjen ska också vägleda ansvariga beställare genom att beskriva vilka kriterier som är styrande vid beslut om att genomföra sourcing.

Införande av sourcing innebär ett strategiskt beslut då det medför påverkan på koncernens driftsmodell för IT. Därför är det viktigt att beslut om sourcing är väl grundat och i linje med koncernens övergripande IT-policy och målarkitekturer.

Riktlinjer för utkontraktering av IT

Vägledning inför beslut om utkontraktering (sourcing)

Inför eventuellt beslut om sourcing ska ansvarig nämnd eller bolag alltid genomföra en förstudie (Ref. Riktlinje för Anskaffning av IT). Beroende på vilken tjänst som omfattas ska förstudien anpassas till den aktuella situationen för att säkerställa ett korrekt underlag för beslut.
I förstudien ska motivet för val av sourcing utvärderas och dokumenteras baserat på områden i tabellen nedan.

Förstudien ska innefatta:

- Bedömning av respektive område med dokumenterade motiv avseende inriktning för eller emot val av sourcing för den aktuella tjänsten.

- Sammanfattande bedömning och motiv avseende inriktning för eller emot val av sourcing baserat på en sammanvägning av alla områden

Område	Underlag för bedömning	Beskrivning
Intern kompetens och förmåga	Vilken kompetens och förmåga finns internt inom koncernen avseende det aktuella området?	Om specifik kompetens och förmåga inom det aktuella området saknas inom koncernen alternativt Fyra Mälarstäder, eller kan vara svår att upprätthålla och bedömningen är att detta istället kan tillhandahållas av en leverantör stärks motivet för sourcing.
Informations-säkerhet	Vilken typ av information ska hanteras i tjänsten och vilka krav på säkerhet ska ställas?	Om bedömningen är att sourcing av den aktuella tjänsten inte innebär en förhöjd informationssäkerhetsrisk, eller om en leverantör bedöms kunna hantera informationen på ett likvärdigt eller bättre sätt ur ett informationssäkerhetsperspektiv stärks motivet för sourcing. För säkerhetsskyddad eller konfidentiell information krävs särskild utredning.
Volym	Är tjänsten en volymtjänst med ett stort antal användare?	Om endast ett fåtal användare ska nyttja tjänsten stärks motivet för sourcing, under förutsättning att leverantören kan tillhandahålla drift, underhåll och support på ett mer effektivt sätt. En volymtjänst som kännetecknas av hög grad av standardisering och flexibilitet kan också vara motiverad att sourca. Volymtjänster med hög grad av verksamhetsunika anpassningar är inte lämplig.
Flexibilitet	Finns behov av hög flexibilitet avseende utformning, förändring och nyttjande av tjänsten?	Om en leverantör kan erbjuda hög flexibilitet genom att snabbt och enkelt anpassa tjänstens utformning, exempelvis genom att flexibelt justera användarlicenser, lägga till eller ta bort funktioner etc. stärks motivet för sourcing.
Bedömd total kostnad	Kan betydande kostnadsbesparingar sett över hela tjänstens livscykel, dvs löpande drift och förvaltningskostnader samt kostnader för upphandling, etablering, utveckling och avveckling uppnås utan att kvalitet och funktionalitet försämras?	Om den estimerade totala kostnaderna bedöms vara lägre vid sourcing jämfört med intern drift, med bibehållen eller högre kvalitet stärks motivet för sourcing.

Styrande principer vid genomförande av sourcing

Vid sourcing av IT ska koncernens riktlinje för anskaffning av IT alltid följas. Nämnder och bolag är ansvariga för att beskriva sina behov och krav, effekter och nytta, genomföra informationsklassning samt risk- och sårbarhetsanalys på en IT- funktion/tjänst/komponent vid sourcing IT.

Avtalet med leverantören ska innehålla tydliga beskrivningar av funktion, kvalitet, tillgänglighet och informationssäkerhet. Avtalet ska även innehålla tydlig beskrivning av ansvarsfördelningen mellan parterna gällande dessa områden:

- Hur leverantören följer kommunkoncernens säkerhetskrav, samt att regelbundna kontroller av IT- och informationssäkerhet genomförs och delges kommunkoncernen.

- Att leverantören har dokumenterade processer för utveckling, drift och förvaltning i enlighet med vedertagen praxis t ex ITIL.

- Hur behörighetshantering behandlas, inklusive hur regelbundna kontroller av behörigheter och IT-säkerhet generellt genomförs och delges kommunkoncernen.

- Var information som hanteras i tjänsten lagras och bearbetas. Leverantören ska informera kommunen om väsentliga ändringar sker avseende lagring.

- Att upphandlande organisation inom Eskilstuna kommunkoncern har exklusiv äganderätt till egen producerad data eller personuppgifter under avtalstiden. Ägandet ska även omfatta kopior av data, inklusive säkerhetskopior.

- All data och information som hanteras inom ramen för sourcingavtalet ska återlämnas till Eskilstuna kommunkoncern i samband med avveckling av tjänst. Data som ska bevaras eller överföras till annat system ska ha ett kompatibelt standardiserat format för att säkerställa överföringen.

- Tjänster som hanterar data enligt en högre informationssäkerhetsklassning ska kunna erbjuda krypterad lagringsarea samt loggning av definierade händelser.

- Att koncernen ska ha möjlighet att genomföra granskningar av leverantören och dess underleverantörers verksamhet, inklusive säkerhetsgranskningar av oberoende part.

- Vid upphörande av tjänst ska leverantören eliminera och radera alla spår av data tillhörande Eskilstuna kommunkoncern och som lagrats hos leverantören, efter godkännande av objektsägare/objektsledare.

- Ett personuppgiftsbiträdesavtal ska alltid tecknas vid utkontraktering av tjänst som hanterar personuppgifter oavsett art.

Följande styrande principer gäller för koncernens interna hantering i samband med sourcing.

- Vid nyttjande/anskaffning av utkontrakterade tjänster, exempelvis molntjänster ska tydliga roller och ansvar anges för att hantera leverantörsrelationen i enlighet med etablerade rutiner.

- Leverantören får inte utan beviljat tillstånd av behörig person inom koncernen ges tillgång till koncernens huvudkatalog för IT (Active Directory - AD).

Ansvar vid sourcing av IT

Nämnderna och bolagen är ansvariga för att denna riktlinje efterlevs i den egna verksamheten.

IT-chef/IT chef bolagen (CIO) ansvarar för kommunens och bolagskoncernens infrastruktur samt målarkitekturer och har utifrån detta mandat att påverka kravställning i samband med sourcing.

Serviceförvaltning IT och ESEM IT ansvarar för att tillsammans med upphandlingsenheten kravställa, utvärdera samt teckna samtliga IT relaterade avtal, enligt gällande delegationsordning. Vidare ansvarar SEF IT för återrapportering till respektive objektsförvaltning avseende licensnyttjande i kommunen.

Upphandlingsenhet ansvarar för att kommunens övergripande riktlinjer för inköp och upphandling samt att gällande produktgruppsstrategier efterlevs.

EA-funktion inom kommun och bolagen, den strategiska arkitekturfunktionen för IT, ansvarar för att koncernens målarkitekturer efterlevs och har mandat att påverka kravställning i samband med sourcing av IT.

Uppföljning

Ansvar för efterlevnad och därmed även uppföljning av denna riktlinje ligger på respektive förvaltningschef samt på bolags-VD. Ett särskilt ansvar för den gemensamma uppföljningen ligger även på IT-chef inom kommun och bolag. Uppföljning ska ske årligen i samband med bokslut.

Gällande lagstiftning och annan rättslig reglering

- Lag (2016:1145) om offentlig upphandling (LOU)
- Dataskyddsförordningen (GDPR)

Förhållande till redan fattade politiska beslut

Styrande IT-dokument

- IT-policy för Eskilstuna kommun; KSKF/2020:187
- Riktlinjer för upphandling och inköp; KSKF/
- Riktlinje för anskaffning av IT; KSKF/2020:189

Andra styrande dokument som påverkar anskaffningsprocessen/utkontraktering

- Plan för informationssäkerhet; KSKF/2012:346
- Riktlinje och anvisning för uppföljning och insyn av verksamhet som bedrivs av privata utförare 2019-2022; KSKF/2019:45

Informationshantering

- Stadsarkivets rekommenderade arkivkrav för IT-system i Eskilstuna kommun KFN/2020:74

Ordlista för IT-policy, Plan för Eskilstuna kommunkoncerns IT-utveckling, Riktlinje för anskaffning och Riktlinje för utkontraktering

IT: Informationsteknologi, Informationshantering (VAD) och teknik (HUR) i ett gemensamt begrepp.

IT- verksamhet: avses alla IT-relaterade funktioner och IT-relaterat arbete inom Eskilstuna kommunkoncern oavsett om det är inom kärnverksamhet, Digital transformation, IT-organisation inom SEF eller kommunala bolagen samt externa partners.

IT-Funktion: är en organisatorisk del inom kommunala förvaltningen och kommunala bolagen som ansvarar för infrastruktur, drift, support, utveckling gällande IT. Leveranserna sker i form av tjänster som kan vara valbara eller ej valbara (gemensam infrastruktur).

IT-styrning: Handlar om hur man styr IT-verksamhet i organisationen som helhet.

IT-beslut: Beslut som rör IT-styrning. Kan gälla policy eller anskaffning och berör oftast gemensam infrastruktur eller säkerhetskrav.

IT-arkitektur: Arkitekturen beskriver vilka komponenter som ingår i systemet, vad komponenterna ska göra, hur de fungerar ihop samt hur hårdvara och användare påverkar systemet.

IT-Infrastruktur: All hårdvara, mjukvara, nätverk, anläggningar, etc., som krävs för att utveckla, testa, leverera, övervaka, kontrollera eller stödja IT-tjänster.

EA: Enterprise Architekt (Funktion) För att hålla en effektiv helhetsbild utifrån kommunens ambitionsnivå, alltifrån verksamhet till teknik. Detta genom att stödja kärnverksamheten, skapa kontroll över IT frågor och dess vägval samt att vara ett stöd till IT ledningen.

IT-säkerhet: IT-säkerhet är en dels grundläggande hygienkrav som t ex Brandväggar, Antivirus, Logghantering, Back-up, Redundanta driftsplatser och säkra kommunikationsförbindelser (VPN). För det andra så är det en del av informationssäkerheten, som kan ställa andra ytterligare krav på IT-säkerheten t ex fler-faktors-inloggning mm.

IT-stöd: Är de digitala funktioner (system/applikationer) som används i verksamheten IT-stödet kan i sin tur bestå av flera olika underliggande IT-komponenter.

IT-kundtjänst: Är den funktion som man vänder sig till då man antingen har behov av support (användarstöd eller tekniskt stöd). Kundtjänsten hanterar också beställningar av funktionalitet.

IT-komponent: Är tekniska beståndsdelar som tillsammans skapar ett IT-stöd (system/applikation/hårdvara)

IT-drift: är den verksamhet som upprätthåller tekniska funktioner. Det kan ske i den interna IT-verksamheten, extern tjänsteleverantöt eller 3:e part till den interna IT-funktion.

IT- leverans: är det stöd och tjänster levereras eller samordnas av IT-funktionen det kan vara standardtjänster eller paketerade tjänster producerade av IT-funktionen eller 3:e partsleverantörer.

Legacy-system: avses system som inte längre underhålls och utvecklas, antingen av en leverantör eller internt inom koncernen. Ökar det digitala arvet då måste det hanteras med separata anpassade lösningar för att fungera i en modern infrastruktur.

SLA: Service Level Agreement (SLA) avser avtalade servicenivåer mellan beställare och utförare exempelvis avseende driftsäkerhet, lösningstid vid incidenter, kvalitet och kapacitet.

Målarkiterktur: Utifrån IT-infrastrukturens nuläge sätts ett börläge som man ska sträva emot. Börläget definieras som målarkitektur.

Öppna data: Digital och maskinläsbar information som är fritt tillgänglig för alla och som utan särskilda krav får användas, delas och ändras av vem som helst.

Masterdata: Data som är kritiskt i vår organisation för att kunna bedriva det uppdraget som ålagts nämnd eller bolag hanteras kontrollerat och i så få källor som möjligt. Master data kan definieras i olika kategorier, exempel på sådana är Personinformation, Platsinformation, Produkter och uppdrag, Finansiell och organisatorisk struktur eller Referensdata.

Objektsförvaltning: Modell för att effektivt hantera systemförvaltning. En styr- och samverkansmodell som används för förvaltning och verksamhetsutveckling av IT-stöd inom organisationen. Modellens syfte är att knyta verksamheten och IT närmare varandra i en linjeoberoende organisation.

Skugg IT: IT system och tjänster som används inom koncern men som inte stöds eller levereras av IT-funktionen. Detta bidrar till suboptimering, ökade risker och fördyring av vår gemensamma infrastruktur. Eftersom det inte är en del av organisationens infrastruktur och hanteras därför inte inom gällande basöverenskommelser och SLA.