

## STYRDOKUMENT

### Riktlinjer för IT-anskaffning

<b>Beslutad när</b>	2021-02-04 § 15
<b>Beslutad av</b>	Kommunfullmäktige
<b>Diarienummer</b>	KSKF/2020:189
<b>Ersätter</b>	Riktlinje för Eskilstuna kommuns IT-verksamhet KSKF 2017:655.
<b>Gäller för</b>	Samtliga nämnder och bolag
<b>Gäller fr o m</b>	2021-02-04
<b>Gäller t o m</b>	Tillsvidare
<b>Dokumentansvarig</b>	IT-chef Eskilstuna kommun
<b>Uppföljning</b>	

#### 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.

## Ämnesområde och bakgrund

Denna riktlinje är en konkretisering av Eskilstuna kommuns IT-policy och Riktlinje för upphandling och inköp. I riktlinjen beskrivs vilka principer som gäller inom koncernkoncernen avseende anskaffning av IT-relaterade komponenter, system, tjänster och infrastruktur, nedan benämnt IT.

Vid anskaffning av system och tjänster så gäller riktlinjen oavsett om dessa installeras på kommunens servrar, hos en extern leverantör, eller i de fall där de levereras som en molntjänst.

Riktlinjen omfattar alla nämnder och bolag inom koncernen.

## Riktlinjens syfte

Syftet med denna riktlinje är att säkerställa att all IT-anskaffning sker på ett ändamålsenligt och hållbart sätt samt i enlighet med koncernens målarkitektur för IT samt objektsförvaltningsplaner. Riktlinjen ska även vägleda ansvariga beställare genom att beskriva vilka principer som ska följas vid anskaffning av IT.

## Riktlinjer för anskaffning av IT

### Styrande principer för anskaffning

Följande styrande principer ska alltid följas vid anskaffning av IT:

- Anskaffning av IT ska utföras baserat på verksamhetens samlade behov och på ett för koncernen kostnadseffektivt sätt. Andra perspektiv som ska ingå i upphandlingsunderlag är kvalitet, säkerhet, arbetsmiljö samt att även hållbarhetsaspekter ska beaktas.

### Beslut om anskaffning

Beslut om anskaffning av IT fattas i enlighet med beslutad delegationsordning. Inför beslut om anskaffning behöver nedanstående punkter följas:

- Nämnder och bolag är ansvariga för att beskriva sina behov, sina krav, effekter och nytta, genomföra informationsklassning samt risk- och sårbarhetsanalys vid anskaffning av IT.
- Anskaffning av IT ska ske inom ramen för kommunens och bolagens objektsförvaltning, . Vid anskaffning av verksamhetssystem ska dessa alltid inkluderas i befintligt förvaltningsobjekt.
- All ny anskaffning av IT, som inte avser befintliga avtalade tjänster, ska godkännas av arkitektfunktion (se beskrivning under rubriken ansvar) för att säkerställa att anskaffning sker med beaktande av kommunens och bolagens målarkitektur och infrastruktur för IT.

- Innan anskaffning av IT genomförs ska befintliga lösningar inom koncernen övervägas för att se om identifierat behov kan tillgodoses. Om befintliga lösningar inom koncernen ej kan nyttjas ska i första hand lösningar inom ramen för regionen, Fyra Mälarstäder, eller SKR/Inera övervägas.
- Beställaren har alltid ett ansvar för totalkostnaden d.v.s kostnaden som uppstår i samband med anskaffning, drift och förvaltning samt avveckling.

### **Krav vid anskaffning**

- Anskaffning som inte görs inom ramen för befintliga avtalade tjänster ska inledas med en av beställaren dokumenterad förstudie för beslut om genomförande. Exempelvis ska förstudien innehålla beskrivning av behov, önskemål samt nyttoeffekter.
- En risk- och konsekvensanalys för informationshantering ska genomföras. Om personuppgifter ska hanteras i ett nytt system eller en ny tjänst ska det först säkerställas att behandlingen är tillåten enligt gällande Dataskyddsförordning.
- Anskaffning av IT ska uppfylla de säkerhetskrav som framgår av styrande och stödjande dokument för informations- och IT-säkerhet.
- Vid anskaffning av verksamhetssystem ska en plan för livscykelhantering upprättas som omfattar alla faser mellan planering, avveckling och arkivering.
- Totalkostnaden samt kostnadsansvar ska klargöras inför anskaffning.
- Anskaffning av IT ska utföras med beaktande av gällande lagar och förordningar, såsom Lagen om offentlig upphandling (LOU), Arkivlagen, Dataskyddsförordningen (GDPR) med flera.

### **Hantering av licenser**

Alla programvaror och användarlicenser ska hanteras korrekt och i enlighet med god praxis i syfte att säkerställa att licensvillkor efterlevs samt att koncernen inte betalar för fler licenser än nödvändigt. Därför är det viktigt:

- Att antalet användarlicenser i ett system eller tjänst inte överstiger vad som bedöms vara nödvändigt.
- Att varje användare har ett unikt individuellt användarkonto, med tillhörande lösenord som uppfyller kommunens och/eller bolagens krav.
- Att det finns en etablerad process för att följa upp licensnyttjandet för respektive system eller tjänst.

## Prioritetsordning vid anskaffning av nya IT-system och tjänster

I samband med anskaffning av nya system eller tjänster ska nedan prioritetsordning alltid beaktas.

1. Välj system och tjänster som redan finns internt inom koncernen.
2. Anskaffning av standardiserade system och tjänster.
3. Utveckla system eller tjänst tillsammans med leverantör. Detta ska endast göras i undantagsfall om en tjänst inte finns på marknaden, eller om det behöver göras vissa anpassningar i befintlig tjänst.
4. Utveckla system eller tjänst internt inom koncernen. Detta ska endast göras i undantagsfall om en tjänst inte finns på marknaden och om utvecklingen bedöms vara mindre omfattande.

## Roller och ansvar

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

**IT-chef i Eskilstuna kommun** är ägare av denna riktlinje. **IT chef Eskilstuna kommun och IT chef för bolagen/koncernen** ska tillsammans förvalta, revidera och följa upp efterlevnad av riktlinjen på en övergripande nivå

**Serviceförvaltningen IT (SEF IT)** och **ESEM-IT** ansvarar för att tillsammans med upphandlingsenheten (eller bolagens motsvarighet) kravställa, utvärdera samt teckna samtliga avtal relaterade till IT-infrastruktur, enligt gällande delegationsordning. Vidare ansvarar SEF IT och ESEM- IT för återrapportering till respektive objektsägare avseende licensnyttjande.

**Upphandlingsenheten** ansvarar för att denna riktlinje tillämpas i upphandlingsprocessen.

**Arkitekturfunktionen** för IT inom kommunen och bolagen, ansvarar för kravställningen på koncernens målarkitektur efterlevs i samband med anskaffning av IT.

## Uppföljning

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

## **Gällande lagstiftning och annan rättslig reglering**

- Lag (2016:1145) om offentlig upphandling (LOU)
- Dataskyddsförordningen (GDPR)
- Arkivlagen (1991:782)
- Lag (2018:1937) om tillgänglighet till digital offentlig service

## **Förhållande till redan fattade politiska beslut**

Nedanstående styrande dokument har en påverkan på anskaffningsprocessen.

- IT-policy för Eskilstuna kommun; KSKF/2020:187
- Plan för Eskilstuna kommunkoncerns IT-utveckling, KSKF/2020:188
- Riktlinje för upphandling och inköp; KSKF/2019:67
- Plan för informationssäkerhet; KSKF/2012:346
- Riktlinjer för behandling av personuppgifter; KSKF/2018:47
- Riktlinje för utkontraktering av IT; KSKF/2020:190
- Stadsarkivets rekommenderade arkivkrav för IT-system i Eskilstuna kommun KFN/2020:74

## **Ordlista för IT-policy, Plan för Eskilstuna kommunkoncens 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 tjänsteleverantör eller 3:e part till den interna IT-funktionen.

**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.

**Målarkitektur:** 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 linjeberoende 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.