

**Vad ingår i medlemsbidraget**  
**Sydnärkes IT-Förvaltning**

## Innehåll

Bakgrund.....	3
Inledning .....	3
Ändringar i uppdrag.....	4
System, tjänster och arbetssätt .....	5
Inköp av enheter.....	5
Applikationer och verksamhetssystem.....	6
Molntjänster och Software as a service (SaaS) .....	7
Microsoft 365 (M365).....	7
Digitalisering och AI .....	8
IT- och Informationssäkerhet .....	8
System för ärendehantering.....	9
Driftmeddelanden .....	9
Incidentrapportering .....	9
Arbetssätt .....	9
Dataskommunikation och fastigheter .....	10
IT och relation med fastighetsägare .....	11
Installationer i fastighet.....	11
Reservkraft, kyla och brandskydd.....	11
Ekonomi, fakturering och investeringar .....	11
Bilaga 1 Krav och funktionsbeskrivning för IT-support.....	13
Bilaga 2 Samverkan.....	16
Bilaga 3 Tjänstebeskrivningar .....	19
Klienthantering .....	19
Applikationsdrift .....	21
Nätverk .....	24
Datacenter och serverdrift .....	25
Bilaga 4 Termer och förkortningar.....	27

## Bakgrund

Askersunds kommun, Hallsbergs kommun, Laxå kommun och Lekebergs kommun har sedan 2014 samverkat kring IT.

Medlemsbidragens storlek beräknades vid nämndens bildande utifrån då gällande respektive medlemskommuns dåvarande IT-budget och har sedan dess justerats främst med bäring på kostnadsökningar avseende löner, licenser och hyreskostnader. Förändringen i budget justeras årligen baserat på individuella kapitalkostnader samt gemensamma kostnader. De gemensamma kostnaderna fördelas enligt invånarantal det senaste hela året före budgetåret.

Sedan IT-nämnden bildades har medlemskommunernas verksamheter växt relativt vilket påverkar IT-förvaltningen på flera sätt, dels har antalet användare och antal klienter (datorer, surfplattor, mobiltelefoner) ökat, dels att det har tillkommit nya verksamhetsställen vilket innebär ökat behov av nätverk och kommunikation (nätverksutrustning i form av switchar och accesspunkter för wi-fi samt att det tillkommer fler verksamhetssystem och applikationer att drifta och förvalta).

Detta dokument syftar till att tydliggöra vad som ingår i det befintliga medlemsbidraget.

Ansvarig för revidering är förvaltningschef IT, i samråd med kommunchefer/kommundirektörer i medlemskommunerna.

## Inledning

IT-förvaltningen ansvarar för att, i samarbete med verksamheterna och upphandling, hantera de avtalsområden som ingår i medlemsbidraget. Dessa områden omfattar främst de system där IT fungerar som systemägare, vilket inkluderar den tekniska IT-infrastrukturen (mer detaljer i nästa stycke). I ansvaret ingår Askersunds kommun, Hallsbergs kommun, Laxå kommun, Lekeberg kommun, Lekebergsbostäder, Lekebergs kommunfastigheter, Hallsbergs bostads AB, Laxåhem, Laxå Kommunfastigheter, Laxå vatten, Laxå värme och Sydnärkes kommunalförbund.

IT-förvaltningen är tillsammans med verksamheterna ansvarig för att säkerställa att det finns ett sortiment anpassat för verksamheternas behov av exempelvis arbetsplatsdatorer, skol- och elevdatorer samt mobiltelefoner och surfplattor. Vid val av IT-utrustning tar IT-förvaltningen fram underlag och rekommendationer som samverkas i IT-dialogforum (bilaga 2). Val av enheter till skola och utbildning görs i samverkan mellan IT-förvaltningen och utvalda representanter från skola och utbildning.

För övrig IT-utrustning tillhandahåller IT-förvaltningen en webshop, där produkter som skärmar, tangentbord, telefoner och skal kan beställas av verksamheten själva. Sortimentet som erbjuds är begränsat och bestäms av kommunerna tillsammans med IT-förvaltningen utifrån verksamhetens behov. Detta sker i IT-dialogforum.

IT-förvaltningens kompetenser är nödvändiga vid verksamheternas upphandlingar. IT-förvaltningen måste ha en representant från upphandlingsprocessens start. Ingen IT-relaterad upphandling får initieras utan IT-förvaltningens medverkan.

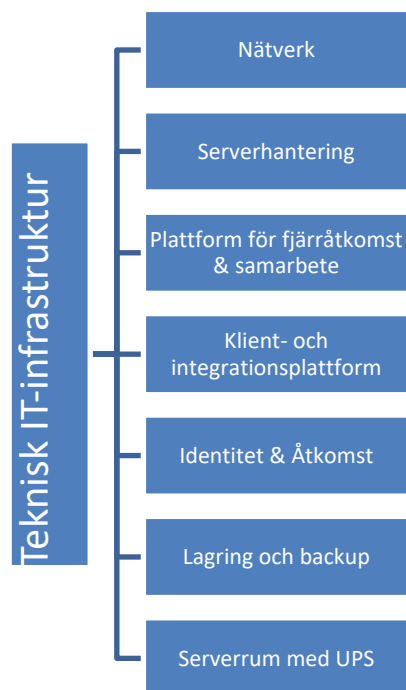
IT-förvaltningen ska även stödja de utvecklingsuppdrag och digitaliseringsinitiativ som prioriteras, och fungera som ett stöd för verksamheterna i det dagliga arbetet, där IT används som en resurs för att uppnå verksamheternas mål.

Till den tekniska IT-infrastrukturen räknas nätverk (hårdvara och mjukvara för intern och extern kommunikation), plattform för fjärråtkomst och samarbete (Virtual Private Network (VPN), Teams, Email), fysiska och virtuella servrar, klient- och integrationsplattform, Identitet och behörighet (Active Directory (AD)), struktur för lagring (av filer), säkerhetskopieringssystem samt serverrum med

batteribackup UPS (Uninterruptible Power Supply).

IT-förvaltningen är systemägare och förvaltare av den tekniska IT-infrastrukturen. I arbetet ingår proaktivt arbete med IT- och informationssäkerhet i nära samarbete med kommunernas informationssäkerhetsansvariga.

## Teknisk IT-infrastruktur



## Ändringar i uppdrag

Större ändringar i innehållet sker en gång per år eller vid akuta behov (lagändring).

Ekonomiska förändringar av medlemsbidraget bereds av IT-nämnd och på budgetdag. Sker i dialog med Kommunchefer och Kommundirektörer (KC/KD), men beslutas av respektive kommuns kommunfullmäktige i samband med budgetbesluten.

Organisationsförändringar sker, efter dialog med/information till KC/KD och samverkan med fackliga organisationer, genom beslut i Sydnärkes IT-nämnd.

Strategiska val som påverkar organisation eller budget lyfts till KC/KD för beslut, för att slutligen föras vidare för beslut till Sydnärkes IT-nämnd.

Strategiska val kopplade till den tekniska IT-infrastrukturen som inte medför organisatoriska förändringar för IT-förvaltningen eller budgetpåverkan kan fattas av förvaltningschef IT. Exempel på sådana beslut är val av virtualiseringsplattform och server- och nätverksarkitektur.

IT-miljöer utvecklas ständigt genom ett kontinuerligt och nära samarbete mellan IT och verksamheterna enligt samverkansmodellen för digitala tjänster. Alla förändringar av IT-miljön som inte ryms inom medlemsbidraget ska hanteras inom budgetprocessen.

Mindre utvecklingsärenden hanteras inom ramen för Förvaltningschefens mandat.

Utvärdering av ny teknik, så kallade pilotprojekt, som kan hanteras med befintlig budget, ska passera KC/KD som ett utvecklingsärende. Detta gäller både för IT och för övriga verksamheter.

Vid förändrade omständigheter, såsom yttre hot, nya regulatoriska krav, ändringar i licensavtal eller krav på förnyelse av IT-utrustning och system på grund av att de inte längre stöds eller tillverkas, vilket kan medföra betydande ekonomiska konsekvenser, kan en justering av medlemsbidraget bli nödvändig. Detta för att säkerställa fortsatt tillgång till en tillgänglig, säker och pålitlig teknisk infrastruktur.

## System, tjänster och arbetssätt

IT-förvaltningen ansvarar, i samarbete med verksamheterna och stöd av upphandling, för att hantera de avtalsområden som ingår i medlemsbidraget, vilket säkerställer att rätt system och tjänster tillhandahålls för att stödja både IT och verksamheternas mål. IT har ansvar för att utveckla arbetssätt och rutiner för de system och tjänster som faller under den tekniska IT infrastrukturen, medan verksamheterna ansvarar för att utforma arbetssätt och rutiner för sina egna system och tjänster. När det gäller gemensamma system/tjänster ska IT och verksamheterna samarbeta för att skapa effektiva arbetssätt och rutiner. Samverkan mellan verksamhet och IT sker enligt samverkansmodellen för digitala tjänster (bilaga 2).

## Inköp av enheter

IT-förvaltningen erbjuder ett definierat utbud av datorer, mobiltelefoner och surfplattor. Detta utbud förvaltas av IT utifrån arbetet i IT-dialogforum. All sådan utrustning ska införskaffas via IT-förvaltningen, om inte ska inköp via andra kanaler godkännas. För utrustning som anskaffats utanför fastställd process kan IT-förvaltningen exempelvis vidta åtgärder som att: neka anslutning till nätverket för icke-godkänd utrustning, avvisa support- och serviceärenden för berörd utrustning, kräva att enheten returneras och ersätts med godkänd utrustning, samt kräva att verksamheten själv står för eventuella merkostnader för support och underhåll.

Vid val av utrustning ska utrustning med en längre livstid prioriteras framför utrustning med kortare kalkylerad livslängd (tillverkarens standardgaranti). Detta för att uppnå en balans mellan konsekvens för miljö och konsekvens för ekonomi.

Datorarbetsplats (stationär/bärbar), skrivare/kopiatorer, skärmar ska väljas utifrån krav på en teknisk livslängd av minst fyra år.

Skrivare/kopiatorer erbjuds/köps in av respektive verksamhet via ADDA och ramavtalet.

Skärmar och tillbehör köps in av respektive kommun genom tillhandahållens webshop.

I medlemsbidraget ingår leverans av datorarbetsplats och elev/skoldatorer/surfplattor, åldersutbyte och återlämningsprocess för återvinning/återbruk. Vid åldersutbyte hanterar IT endast återvinning av dator, mobiltelefoner och surfplattor. Övrig teknisk utrustnings återvinning hanterar verksamheterna själva. PC, MAC, och surfplattor köps in via IT-förvaltningens investeringsbudget som tas fram med respektive kommun och baserat på dialog med berörda verksamheter. Avskrivningstiden för PC och MAC är fyra år. För surfplattor är det tre år. Planerad livslängd för MAC och surfplattor är sex år och för PC fyra år. All specialutrustning, mobiltelefoner och övrig arbetsplats relaterad utrustning beställs av verksamheten genom tillhandahållens webshop och respektive verksamhet faktureras direkt.

## Audiovisuell (AV) teknik/utrustning

Verksamheterna ansvarar för inköp, installation och drift av audiovisuell utrustning. IT-förvaltningen tillhandahåller en inköpsmöjlighet via det nuvarande IT-partneravtalet, där verksamheterna kan välja att köpa AV-utrustning antingen från nuvarande IT-partner eller från en av IT-partners underleverantörer.

Vid val av IT-partner som leverantör kan verksamheterna beställa AV-utrustning via tillhandahållens webshop. Vid val av underleverantör sker beställningar via leverantörens egna kanaler. Verksamheterna står fria att välja vilken AV-utrustning och vilket supportavtal som passar deras behov. Om verksamheterna inte önskar använda IT-partneravtalet är alternativet en egen upphandling av AV-utrustning och tillhörande tjänster.

Både inköp och tecknande av supportavtal hanteras och bekostas av verksamheterna själva, oavsett vilken inköpsväg som väljs. Verksamheterna ansvarar även för uppsättning och montering av utrustningen, antingen i egen regi eller genom att beställa installationstjänster från leverantören.

IT-förvaltningen ska dock alltid rådfrågas i följande fall:

- När utrustningen behöver anslutas till wifi
- När licenser krävs för utrustningen
- Vid utskick/installation av applikationer på klienter (PC/Mac/surfplattor)

Alla inköp av utrustning och teknik som ska kopplas in på eller kommunicera med den IT-tekniska infrastrukturen ska hanteras av IT-förvaltningen eller ske med IT-förvaltningens kännedom och godkännande.

## Garanti

IT tillhandahåller en hårdvarugaranti på datorarbetsplats. Garantiärenden för elev/skoldatorer och surfplattor hanteras av respektive kommun själva inklusive vilka försäkringar som tecknas. Garantiärenden på produkter från tillhandahållen webshopen hanteras av användaren själva direkt via webhoppen.

## Applikationer och verksamhetssystem

IT-förvaltningen ska vara delaktig vid införandet av nya verksamhetssystem för att säkerställa att implementeringen och driften sker på ett säkert sätt. Alla inköp och förändringar av verksamhetssystem som har beroende/påverkan av/på den tekniska IT-infrastrukturen ska godkännas av IT-förvaltningen.

IT-förvaltningen ansvarar för den tekniska systemförvaltningen, förutsatt att det inte är en molntjänst eller att inget annat har överenskommits mellan verksamhet och IT-förvaltningen. Verksamheten ansvarar för den verksamhetsbaserade systemförvaltningen. Ansvaret fördelas i samråd mellan verksamhet och IT.

För vissa verksamhetssystem har IT-förvaltningen kompetens att genomföra uppdateringar i egen regi. För övriga verksamhetssystem där leverantörskonsult krävs för uppgradering, felsökning eller annan teknisk support, står verksamheten för konsultkostnaderna om inget annat är överenskommet. Denna ansvarsfördelning ska dokumenteras i objektplanen där respektive verksamhetssystem ingår.

Samtliga informationssystem/verksamhetssystem som används eller planeras att användas i av verksamheterna ska även informationsklassas av verksamheten. Klassningen avgör vilken säkerhetsnivå och vilket säkerhetsskydd som systemet ska ha. Skyddet ska utvecklas i samråd mellan verksamhet och IT-förvaltningen. Rekommendationen är att informationsklassning samordnas i objekten enligt samverkansmodellen för digitala tjänster (bilaga 2).

Teknisk systemförvaltning är en viktig del av den övergripande systemförvaltningen och fokuserar specifikt på de tekniska aspekterna av att underhålla och utveckla IT-system. Här är en översikt av vad teknisk systemförvaltning innebär:

**Teknisk systemförvaltning, även kallad applikationsdrift innebär:** övervakning och hantering av applikationer enligt instruktioner fastställda i samråd med systemförvaltare och/eller applikationsleverantör. Ansvaret inkluderar även incidenthantering, problemhantering och ändringshantering av verksamhetsapplikationen.

Se bilaga Applikationsdrift för detaljer.

Innan applikationsdrift implementeras för en ny applikation är det viktigt att verksamheten och IT-förvaltningen har en gemensam överenskommelse. IT kan avböja applikationsdriftsansvar på grund av exempelvis resurs- och kompetensbrist, hög risknivå, säkerhetsrisker, eller oklara roller och ansvar. I sådana fall kan IT rekommendera eller föreslå en annan leveransmodell, såsom molntjänst eller att

leverantören ansvarar för applikationsdriften och IT ansvarar för serverdriften.

Ifall applikationsdrift ska implementeras behöver följande variabler levereras av applikationsleverantören och verksamheten:

Applikationsdokumentation.

Driftdokumentation med åtgärder som skall utföras vid avvikelser.

Tillgång till en portal för nedladdning av uppdateringar och registrering av ärenden hos leverantören.

För applikationer som använder sig av den tekniska IT-infrastrukturen men som inte förvaltas av IT-förvaltningen gäller endast serverdriftsansvar:

**Serverdrift** innebär underhåll, konfiguration och optimering av servrar för att säkerställa att de fungerar effektivt och ändamålsenligt för en verksamhet.

#### Huvuduppgifter:

- Uppsättning av servrar i datacenter.
- Installation och konfiguration av operativsystem som exempelvis Windows Server.
- Övervakning av serverns funktioner och prestanda, inklusive CPU-användning, diskanvändning och nätverkstrafik.
- Säkerhetshantering, vilket innefattar installation av säkerhetspatchar, övervakning av säkerhetsloggar och konfigurerings av brandväggar.
- Hantering av säkerhetskopior för att skydda mot dataförluster samt löpande säkerhetskopiering.
- Programuppdateringar och optimering av serverns prestanda.

Det blir allt vanligare att systemleverantörer erbjuder molntjänster, men det finns fortfarande behov av kopplingar till den tekniska IT-infrastrukturen, exempelvis för inloggning och integrationer mot användarregister och andra system.

#### Molntjänster och Software as a service (SaaS)

Vid övergång till molntjänst eller SaaS är det viktigt att IT och verksamheten samarbetar. Innan en förändring genomförs så måste flertal aspekter så som säkerhet och juridik granskas och tas i beaktning, vilket kan göras genom en informationsklassning och riskanalys. Exempel på frågeställningar som verksamheten behöver besvara:

**Säkerhet:** Säkerställa att leverantören uppfyller krav på dataskydd och integritet.

**Juridiska:** Kontrollera att leverantören följer lagar och regler, som GDPR. Undersöka var data kommer att lagras och att det följer juridiska krav.

**Verksamhetsbehov:** Kontrollera att molntjänsten har tillräcklig prestanda och tillgänglighet för att möta verksamhetens behov. Tydliggöra vem som äger och kontrollerar data, samt hur man får tillgång till och kan exportera data vid byte av leverantör.

**Ekonomi:** Genomföra en kostnadsanalys som inkluderar både direkta och indirekta kostnader, inklusive driftskostnader, licenser, och eventuella interna kostnader för att hantera tjänsten. Ett system kan innebära interna kostnader även om det driftas externt hos leverantören.

#### Microsoft 365 (M365)

I medlemsbidraget ingår licenser för M365. Dessa är valda utifrån krav på säkerhet samt typ av användare: personal med egen dator, personal med delad dator, skolpersonal samt elever. Behov av förhöjd licens beviljas av chef då det kan innebära ökade kostnader.

Övriga licensköp som är kopplade till M365 utifrån ett verksamhetsbehov betalas av verksamheten, till exempel Power BI och Co-Pilot.

## Digitalisering och AI

Digitalisering drivs av verksamheten själv, med stöd från IT-förvaltningen.

Verksamheten har ansvaret för:

- Att identifiera behov och möjligheter
- Att leda förändringsprojekt
- Att sätta mål och prioriteringar
- Att säkerställa att digitaliseringen skapar verksamhetsnytta

IT-förvaltningen bistår med teknisk rådgivning och är behjälplig med att utvärdera tekniska lösningar samt ge input kring tekniska möjligheter och begränsningar.

Verksamheterna är ansvariga för framtagning av AI-vision/strategi/policy som konkretiserar vad verksamheten vill uppnå med AI och tydliggör hur AI ska stödja och användas av olika intressenter som exempelvis:

- Medarbetare
- Medborgare
- Organisation/verksamhet
- Ledning/styrelse

IT-förvaltningen bistår med teknisk rådgivning och är behjälplig med att utvärdera AI lösningar samt ge input kring tekniska möjligheter och begränsningar.

## IT- och Informationssäkerhet

I dagens digitaliserade värld blir skillnaden mellan IT-säkerhet och informationssäkerhet alltmer relevant att förstå. Dessa två områden är nära besläktade men har olika fokus och ansvarsområden som tillsammans skapar ett heltäckande skydd för organisationer.

**IT-säkerhet** handlar primärt om att skydda systemen och den tekniska IT-infrastrukturen.

**IT-förvaltningens ansvar:**

- Ansvar för tekniska skyddsåtgärder för system och data som exempelvis brandväggar, virusskydd och säkerhetsuppdateringar
- Hantering av identitets- och åtkomsthantering
- Övervakning och skydd mot cyberattacker

IT-säkerhet utgör därmed det tekniska skyddsnätet som förhindrar obehörig åtkomst och skyddar mot direkta hot mot systemen.

**Informationssäkerhet** har ett bredare perspektiv och omfattar alla aspekter av hur information hanteras, oavsett om den är digital, fysisk eller muntlig:

- Bredare perspektiv som omfattar all information oavsett format
- Hantering av riktlinjer, policyer och processer kring informationshantering
- Inkludering av fysisk säkerhet, personalutbildning och medvetenhet
- Fokus på konfidentialitet, integritet och tillgänglighet av information

**Verksamhetens ansvar:**

- Ägande av informationen och definition av dess värde
- Beslut om informationsklassificering
- Upprätta en informationssäkerhetspolicy samt följa upp efterlevnaden
- Definition av verksamhetskrav för IT-system och säkerhet



Informationssäkerhet handlar således om att skydda informationens värde genom hela dess livscykel, från skapande till arkivering eller gallring.

För att uppnå en effektiv säkerhetsnivå krävs tydlig kommunikation och samarbete mellan IT och verksamheten. Detta samarbete skapar en balans där tekniska lösningar implementeras baserat på verksamhetens behov och informationens känslighet. IT-förvaltningen bistår med vägledning om tillgängliga tekniska lösningar. I slutändan bär båda parter ett gemensamt ansvar för att skydda verksamheternas värdefulla informationstillgångar och system.

IT-förvaltningen ansvarar även för att besvara IT-relaterade frågor från externa parter, exempelvis revision, eller bistår verksamheten när sådana frågor inkommer.

## System för ärendehantering

Det ärendehanteringssystem som IT använder för ärendehantering kan även användas av andra verksamheter vid behov. Detta förutsätter dock överenskommelser med IT kring resurser och kostnader. IT är systemägare för systemet. Alla kommunens användare kan registrera ärenden i ärendehanteringssystemet.

## Driftmeddelanden

IT-förvaltningen ska använda kommunernas respektive Intranät (eller den plats som kommunerna anvisar) som plats för sin information gällande driftinformation. Driftmeddelanden syftar till att säkerställa transparens och ge användare eller verksamheter möjlighet att planera sitt arbete utifrån aktuell driftstatus. Kommunens kommunikatör stöttar IT-förvaltningen med att skapa och formulera driftinformation.

Det finns två typer av driftmeddelanden:

**Planerade driftmeddelanden:** Dessa meddelanden informerar om kommande underhåll eller servicearbeten som är schemalagda i förväg. De är viktiga för att användare och verksamheter ska kunna förbereda sig för eventuella avbrott.

**Oplanerade driftmeddelanden:** Dessa meddelanden ges vid oförutsedda driftstörningar, som kan bero på tekniska fel eller skador på utrustning. De informerar användare och verksamheter om att det finns ett problem och ger ofta en uppskattning av när tjänsten kan återställas.

## Incidentrapportering

IT-förvaltningen ska dokumentera och rapportera en IT-incident enligt en strukturerad och tydlig process. För allvarliga eller återkommande incidenter ska en root cause analysis (RCA) genomföras för att identifiera grundorsaken och vidta åtgärder för att förhindra att den upprepas. Verksamheterna rapporterar incidenter för sin verksamhet.

## Arbetsätt

IT-förvaltningen har kompetens att hantera frågor inom IT-arbetsplats, där hanteras exempelvis teknisk support för datorer och mobila enheter samt användarrättigheter och behörigheter. På IT-infrastruktur arbetar man bland annat med drift av nätverk, servrar och brandväggar.

Inom IT-förvaltningen finns även objektledare IT, vars huvudsakliga uppgift är att arbeta med samverkan enligt den gemensamma samverkansmodellen för digitala tjänster.

Första linjens support är den generella supporten med bred kunskap som hanterar all inkommande förfrågan om support från verksamheterna. IT arbetsplats ansvarar för servicedesk.

Andra linjens support, ärenden som kräver djupare support, hamnar hos IT arbetsplats eller IT

infrastruktur. Det kan vara ärenden som kräver längre handläggningstid eller besök på plats.

Tredje linjens support är för ärenden som kräver mer specifik expertis när det gäller stöd till användare och felsökning av verksamhetssystem, infrastruktur och gemensamma plattformar. Denna typ av ärenden hanteras både av IT arbetsplats och IT infrastruktur.

IT arbetsplats och IT Infrastruktur ansvarar för underhåll och utveckling av den tekniska IT-infrastrukturen samt samarbetar med objektledningen för att hantera IT-säkerhetsfrågor.

Objektledning består av objektledare IT.

Samverkansmodell för digitala tjänster är baserad på förvaltningsmodellen PM3.

I medlemsbidraget ingår utbildning i modellen, objektledare IT för respektive objekt samt strukturer, processer och dokumentmallar för framtagande av objektplan och löpande uppföljning gällande vidmakthållande och viss vidareutveckling.

Objektplan tas fram årsvis för respektive objekt och ska innefatta objektets behov samt kortsiktiga och långsiktiga mål. Objektledare IT håller i arbetet, vid behov driver på detsamma och bidrar med IT's behov och mål. Verksamheten, i form av objektledare och objektägare, ansvarar för att bidra med verksamhetens behov och mål.

Objektsarbetet ska utgå från verksamhetens behov. Verksamhetens objektledare leder det verksamhetsnära arbetet inom objektet med ansvar för att identifiera behov, säkerställa måluppfyllelse i objektplanen och att IT-stödet ger avsedd nytta samt skapa förankring inom den egna verksamheten. IT översätter verksamhetsbehov till IT-aktiviteter och tar ett helhetsansvar för samordningen av dessa aktiviteter tillsammans med objektledare i verksamheten eller motsvarande

## Datakommunikation och fastigheter

WAN (Wide Area Network) kan delas in i två huvudsakliga kategorier:

1. Grundinfrastruktur WAN
  - Ingår i medlemsbidraget
  - Utgör en grundläggande förutsättning för den tekniska IT-infrastrukturen
  - Täcker den övergripande nätverksstrukturen
2. Verksamhetsspecifik WAN
  - Etableras när en kommunal verksamhet (exempelvis en skola) saknar egen fiberanslutning
  - Utnyttjar Telias fibernät när egen fiber inte finns tillgänglig
  - Medlemsbidraget täcker för närvarande verksamheternas driftkostnad för en standardkapacitet (100Mbit/s)
  - Behov av högre kapacitet medför ökade WAN kostnader vilket kan leda till att medlemsbidraget behöver höjas

- Förutsättning för högre hastighet är stark kopplat till fastighetsnätets\* prestanda, standarder och ålder på exempelvis kablage.

\* Fastighetsnätet består av olika komponenter, inklusive kopparkablar (t.ex. Cat6 eller Cat7) för traditionell data- och telefonkommunikation, samt fiberkablar för att uppnå högre bandbredd och längre överföringsavstånd:

Kostnadsfördelning för fiber och nätverk:

- Etablering och underhåll av fibernät åligger respektive kommun
- Etablering och underhåll av nätverk i byggnader åligger respektive kommun
- Etablering, underhåll och livscykelhantering av aktiv nätverksutrustning som switchar och accesspunkter hanteras av IT-förvaltningen och ingår i medlemsbidraget

Målsättningen är även att skapa en tydlighet kring kostnadsfördelning som säkerställer transparens när en kommun väljer mellan att investera i eget nät eller köpa nätverkskapacitet från extern leverantör.

Uppsättning och utbyte av switchar utförs av IT.

Montering och demontering av accesspunkter utförs av IT. I vissa fall kan fastighetsvärd eller vaktmästare bistå i arbete med montering/demontering av accesspunkter. IT skickar då ut rätt konfiguration till accesspunkten från ett centralt verktyg.

## **IT och relation med fastighetsägare**

En välfungerande samverkan mellan IT-förvaltningen och fastighetsägare är avgörande för driftsäkerheten. Detta gäller särskilt vid:

- Planerade förändringar i fastigheten som kan påverka den tekniska IT-infrastrukturen
- Arbeten inom elområdet som berör IT-utrymmen eller IT-utrustning
- Projekt som kräver teknisk expertis från IT-förvaltningen

Fastighetsägaren ansvarar för att:

- I god tid informera IT-förvaltningen om planerade förändringar
- Bjuda in IT-representanter till relevanta projektmöten
- Säkerställa att förändringar är förankrade med IT-förvaltningen innan genomförande

Genom tidig dialog och tydlig ansvarsfördelning minimeras risken för driftstörningar och andra tekniska problem som kan påverka verksamheterna.

## **Installationer i fastighet**

IT talar om vad för skåp, stativ eller liknande som är lämpligt. IT ska varken montera eller anvisa var fast installation ska ske i byggnad. Detta ansvarar fastighetsägaren för. IT monterar aktiv utrustning i de av fastighetsägaren monterade skåp/stativ.

Kopplingsskåp måste vara utrustade med larm eller lås av flera betydande säkerhetsskäl, såsom skydd mot vandalism och sabotage, samt för att säkerställa att endast auktoriserad personal kan utföra justeringar.

## **Reservkraft, kyla och brandskydd**

Det finns två typer av reservkraftslösningar:

1. Reservkraft via dieselaggregat
  - Placerad på strategisk plats för att säkerställa drift av kritiska system
  - Samtliga aspekter av hantering administreras av kommunen eller dess fastighetsbolag
  - Omfattar:
    - Underhåll
    - Investeringar
    - Avtal
    - Löpande tester
2. Reservkraft via UPS (batterisystem)
  - Dedikerad till utvalda IT-utrymmen
  - Hanteras fullständigt av IT-förvaltningen
  - Ingår i medlemsbidraget

Kylanläggning och brandskydd för IT-utrymmen hanteras av IT-förvaltningen och ingår i medlemsbidraget.

## **Ekonomi, fakturering och investeringar**

IT-förvaltningen upprättar en budget för året som omfattar gemensamma driftkostnader, gemensamma

investeringar samt individuella investeringar, såsom inköp av datorer och accesspunkter. De gemensamma kostnaderna fördelas baserat på invånarantal och de individuella investeringarna budgeteras per kommun utefter prognos på antal utbyten. Dessa kostnader resulterar i ett medlemsbidrag för det aktuella året. Detta bidrag faktureras kvartalsvis. Under löpande år görs uppföljningar, tre prognoser och ett delårsbokslut som redovisas för nämnden och skickas ut till medlemskommunerna. Eventuella underskott eller överskott vid årets slut regleras på den första fakturan för nästkommande år.

Arbetsplatsdatorer budgeteras och kostnadsförs på respektive kommuns individuella investeringar. Kapitalkostnaderna för investeringarna läggs på medlemsbidraget. Avskrivningstiden och den planerade livslängden för datorer är 4 år. Till budget 2026 har medlemskommunerna utökat de individuella investeringarna med att även omfatta accesspunkter. För dessa gäller en avskrivningstid om 5 år. I och med att IT-förvaltningen tagit över ansvaret för inköp och utbyten av accesspunkter, möjliggörs en bättre långsiktig planering.

Gemensamma investeringar får inte överskrida budgeten. Ska större investeringar planeras måste det först godkännas av respektive kommun och därefter föras vidare för beslut till IT-nämnden.

Vid inköp av tillbehör genom tillhandahållens webshopen, såsom headset och USB-minnen, faktureras verksamheterna löpande av leverantören.

Vid stöld på IT-utrustning ansvarar den som har arbetsmiljöansvaret för arbetsplatsen för att informera kommunens säkerhetschef samt göra polisanmälan. Därefter sker en dialog med IT för att avgöra hur stölden ska hanteras.

## Bilaga 1 Krav och funktionsbeskrivning för IT-support

### IT-support

Öppettider helgfria dagar:

Måndag-fredag 07:30–16.00

Vardag före röd dag 07:30–15.00

Alla ärenden ska registreras i ärendehanteringssystemet.

Supportärenden ska i första hand lösas av servicedesk. Om inte går ärendet vidare till andra och tredje linjens support.

Målsättningen är att majoriteten av ärendena ska lösas av servicedesk. IT-förvaltningen följer upp detta internt varje månad och redovisar resultaten kvartalsvis till KC/KD samt IT-nämnden. Resultatet kan även presenteras till verksamheter vid förfrågan.

Handläggningstider för felanmälan gällande "basfunktion" ska om möjligt hålla sig inom en (1) arbetsdag. Servicedesk ska sträva efter att lösa problem så fort som möjligt.

Med "basfunktion" menas att något enligt listan nedan inte fungerar:

- Digital arbetsplats (där Klienttjänst enheten skall starta och man ska kunna logga in)
- Lagringsyta (Behörighet till rätt information utifrån din roll som elev, anställd, förtroendevald, konsult eller liknande, spara, återställning av data etc) Observera att filer inte kan återställas efter en viss tidsgräns har passerat
- Utskrift
- Nätverk
- E-post
- Office applikationer (Word, Excel, PowerPoint, Teams, Onedrive)
- Säker fjärranslutning (VPN-tjänst som möjliggör åtkomst till system och filer vid arbete på distans
- Distribution av programvaror

Vid pågående ärende sker kommunikation genom ärendehanteringssystemet. Vid överenskommelse kan även verksamhet kontakta tilldelad IT-specialist direkt vid ett pågående ärende.

Slumpenkät ska skickas ut till avslutade ärenden för att följa upp användarnöjdheten.

Svaren följs upp internt av IT-förvaltningen. Resultatet kan även presenteras till verksamheter vid förfrågan.

### Supportnivåer

Det finns två olika supportnivåer.

#### 1. Hanterad datorarbetsplats (administrativ och pedagogpersonal och övrig administrativ personal)

För hanterad dator ansvarar IT för hela supportkedjan.

#### 2. Elevdator

För elevdator fördelas ansvaret för supportkedjan:

IT:s åtagande:

- Åtkomst till wifi, nätverk, internet

- Användarens konto och e-post
- Appdistribution

Verksamhetens åtagande:

- Användarstöd
- Påbörja felsökning, samt fortsätta med stöd från IT
- Felanmälan av hårdvara direkt till leverantör
- Reparationer av delar i samråd med leverantör
- Utskrift

## Övriga funktioner/tjänster

### Användarkonto för ej anställd

Användarkonto till personal/person som inte anställs genom Personec beställs via ärendehanteringssystemet via intranätet. Får ansökas av chef.

### Upplägg av funktionsadress

Funktion inom en verksamhet/enhet, som har behov av en direkt e-postadress. Funktionsadresser beställs via ärendehanteringssystem på intranätet. Får beställas av chef eller annan utpekad person.

### Tillgång till programvara utanför standardutbudet

IT skall vara behjälplig med att installera arbetsrelaterade program (program som behövs för att utföra specifika arbetsuppgifter inom en persons yrkesroll och som inte ingår i standardutbud) som saknas i Software Center/företagsportalen. Får beställas av chef eller annan utpekad person.

### Datorarbetsplats (administrativ och pedagogpersonal och övrig administrativ personal)

Debiteras via medlemsbidraget. Förnyas automatiskt med ny hårdvara efter 4år.

### Elevdator/surfplattor

Verksamheten i dialog med IT väljer ut elevdator/surfplattor. Debiteras via medlemsbidraget. Elevdatorer (ej surfplattor) förnyas automatiskt med ny hårdvara efter 4år

### Mobiltelefon och surfplatta

Vid leverans av nya mobiler och surfplattor kommer enheterna vara managerade (styrda/hanterade) via ett tekniskt verktyg (MDM). Detta gör det möjligt för IT att sätta upp konfiguration för åtkomst av nätverk och e-post. Denna typ av support ingår i medlemsbidraget.

Övrig support av applikationer och handhavande ansvarar respektive verksamhet för. Behövs ytterligare support beställs detta från IT genom att skapa ett ärende. Mobiltelefoner debiteras vid inköp via tillhandahållen webshop och abonnemang via respektive kommun. Priser och modellutbud finns på tillhandahållen webshop. Surfplattor beställs via tillhandahållen webshopen och debiteras direkt. Garantiärenden hanteras av verksamheten via tillhandahållen webshopen.

### Skrivare

Respektive kommun ansvarar för inventering av skrivare och beställning sker direkt via leverantörens portal. Inklusiva praktiska frågor som är kopplat till användning av skrivare och Follow-Me hanteras av respektive kommun. Kommunen står för kostnaden för skrivare och tjänsten Follow-Me. IT ansvarar för nätverket och drift av tjänsten Follow-Me. IT behöver informeras vid inköp och utbyte av skrivare. Leverantören ansvarar för hårdvaran. Rekommendationen är att alla skrivare ska använda Follow-Me.

## **Accesspunkt – trådlöst nätverk**

Beställs via ärendehanteringssystemet. Livscykelhantering av accesspunkter hanteras av IT-förvaltningen. Montering och demontering av accesspunkter hanteras av IT. I vissa fall kan fastighetsvärd eller vaktmästare bistå i detta arbete. Rekommenderad förnyelse är efter 5år.

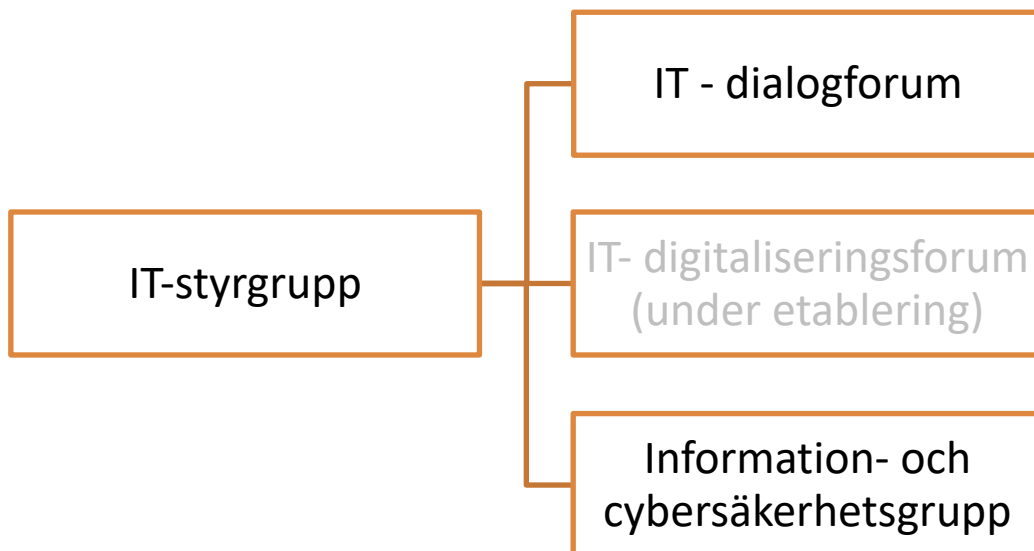
## **Tillbehör**

Exempelvis väskor, fodral, skal, hörlurar mm. Verksamheten beställer via tillhandahållen webshopen och debiteras direkt.

## **Tillgänglighet, underhåll samt förändringsstopp**

Målet är att säkerställa en tillgänglighet för servrar, wifi och integrationsplattform på  $\geq 99,2\%$  per år. IT-förvaltningen ska sträva efter att allt planerat underhåll utförs i överenskommelse med berörd verksamhet. Undantag kan göras för att hantera kritiska säkerhetsbrister eller akuta åtgärder.

## Bilaga 2 Samverkan



Gruppering	Deltagare	Sammankallande
IT - styrgrupp	Kommunchef/Kommundirektör från varje samverkanspart IT-chef	IT-chef
IT - Dialogforum	Adminchefer/Kanslichef	Enhetschef IT
IT - Digitaliseringsforum	Under etablering	Under etablering
Information- och cybersäkerhetsgrupp	Informationssäkerhetsansvarig från varje samverkanspart	Informationssäkerhetsansvarig
Objektstyrgrupp	Objektägare	Objektledare IT

### IT-styrgrupp

IT-styrgruppen träffas fyra gånger per år i anslutning till IT-nämnd. IT-chef sammankallar till mötena.

IT-styrgruppen:

- arbetar med en gemensam målbild för IT-samverkan
- fattar gemensamma beslut med en horisont på 1-5 års sikt och som har en direktpåverkan på den tekniska IT-infrastrukturen
- Förslag kan föras vidare till IT-nämnd för beslut

### IT- dialogforum

IT- dialogforum hanterar gemensamma frågor som uppkommer kring den tekniska IT-infrastrukturen. Vid behov bereder man frågor till IT-styrgrupp för beslut.

IT-dialogforum leds av enhetschef som sätter samman agendan. Anteckningarna ska sparas på överenskommen filyta. Enhetschef bjuder med relevanta roller till mötet utifrån aktuella punkter på



agendan.

Alla deltagare har möjlighet att föreslå diskussionspunkter till mötena. IT-dialogforum sammanträder regelbundet under året, med en kombination av fysiska och digitala möten. Mötestillfällena planeras så att relevanta frågor kan vidarebefordras till IT-styrgruppens sammanträden.

IT-dialogforum:

- Fångar synpunkter på IT's leverans med tyngdpunkt på drift, support samt förändrings/förbättringsbehov
- Är en informationskanal mellan IT och verksamheterna
- Bidrar till samverkan mellan kommunernas verksamheter utifrån den tekniska IT-infrastrukturen

### **Information- och cybersäkerhetsgrupp (ICSG)**

ICSG träffas fyra gånger per år. Mötestillfällena planeras så att relevanta frågor kan vidarebefordras till IT-styrgruppens sammanträden. Informationssäkerhetsansvarig sammankallar till mötena.

Syftet med ICSG:

- Utveckla gemensamma rutiner och arbetssätt inom informationssäkerhet samt fatta beslut inom sitt mandat eller lämnar förslag till rätt beslutsinstans
- Bereda genomgripande frågeställningar kring informationssäkerhet för beslut i IT-styrgruppen och/eller i IT-nämnd
- Är remissinstans och rådgivande i informationsfrågor på ett övergripande plan
- Bidra till samverkan mellan kommunernas verksamheter

Eftersom kommunerna delar en gemensam IT-förvaltning är det viktigt att säkerhetsarbetet samordnas mellan parterna för att kunna ställa enhetliga krav på IT-förvaltningen.

Kommunövergripande frågor behandlas och diskuteras för att fastställa hur de ska tas vidare i respektive verksamhet och organisation. Gruppen kan fatta vissa beslut direkt, medan andra frågor tas vidare till IT-styrgruppen och/eller IT-nämnden för slutligt beslut.

### **Objektstyrgrupp**

Dessa möten hålls på strategisk nivå och inkluderar ledningsrepresentanter från både verksamheten och IT, samt objektledare IT. De hålls ofta två gånger per år och syftar till att fatta beslut om prioriteringar och strategiska vägval.

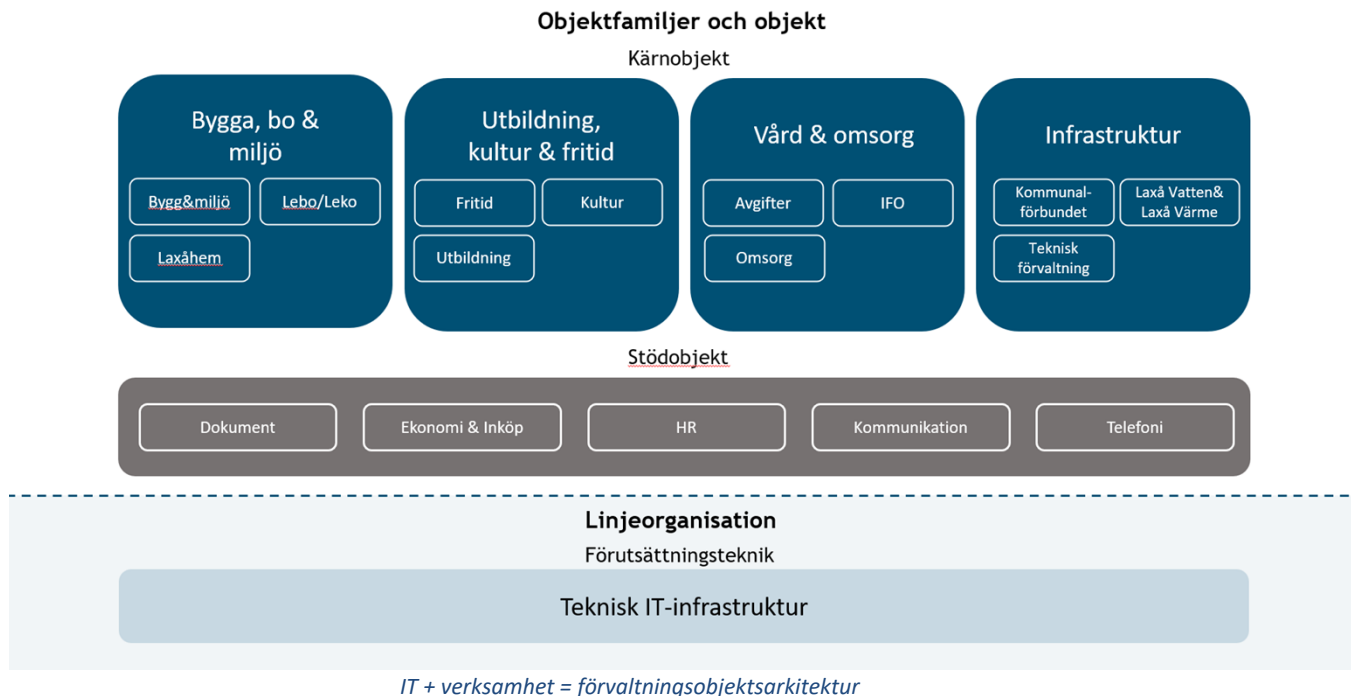
### **Samverkansmodell för digitala tjänster**

För att tydliggöra uppdrag, roller och ansvar för dom digitala resurserna arbetar kommunerna utifrån en gemensam samverkansmodell för digitala tjänster.

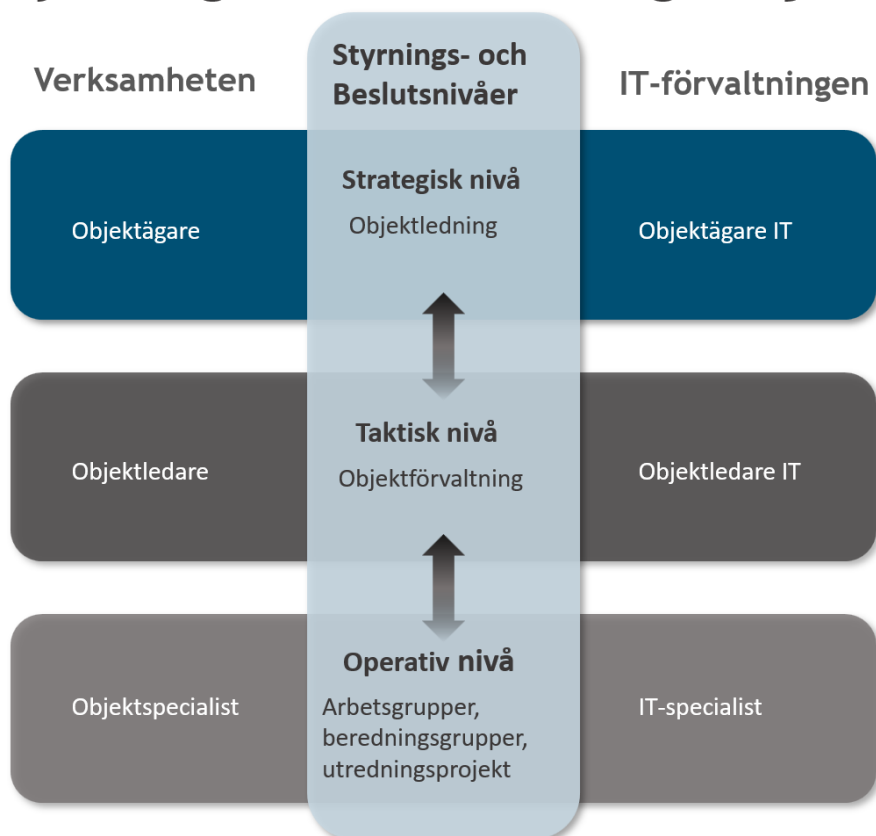
Samverkansmodellen syftar till att skapa en strukturerad och effektiv styrning av digitala resurser genom tydliga roller och ansvar. Målet är att få ut största möjliga nytta av verksamhetssystem och digitala tjänster genom en aktiv och tvärfunktionell förvaltning som:

- Säkerställer att system och tjänster effektivt bidrar till att tillgodose verksamheternas och invånarnas mål och behov
- Tydliggör samverkan mellan IT och verksamhet
- Möjliggör kontroll av systemkostnader
- Ger stöd för de aktiviteter som ska genomföras för att upprätthålla nytta, kvalitet och säkerhet
- Möjliggör att kompetens om både verksamheten och tekniken möts i ett gemensamt uppdrag

## Objektsarkitektur (OA)



## Styrning av förvaltningsobjekt



## Bilaga 3 Tjänstebeskrivningar

### Klienthantering

Tjänsten levereras inom ramen för medlemsbidragen och Sydnärkes IT-förvaltning har som mål att klienthantera alla persondatorer, mobiltelefoner och surfplattor.

Klienthantering underlättar för dig som användare att arbeta på din dator, mobiltelefon eller surfplatta utan att behöva tänka på frågor kring säkerhetsinställningar och uppdateringar, hantering av hårdvara, operativsystem, drivrutiner och licenser (M365 licenser).

Med hjälp av klienthantering kan man även säkerställa att din enhet är korrekt konfigurerad för att motverka IT- och andra säkerhetsincidenter. Klienthanteringen hjälper dig att hålla datorns operativsystem och programvaror uppdaterade samt inkluderar ett komplett virussydd. Vissa klientplattformar har dessutom utökade funktioner för att hantera eventuell stöld eller förlust av din enhet.

#### Exempel på hantering som ingår:

**Installation och konfiguration:** Distribuering av operativsystem och applikationer samt konfiguration av nya enheter.

**Underhåll och uppdateringar:** Löpande system-och säkerhetsuppdateringar.

**Felsökning och support:** Identifiering och lösning av problem relaterade till klientenheter.

**Säkerhet:** Implementering av säkerhetspolicies som antivirus, brandväggar och kryptering.

**Klienttjänsten** omfattar följande komponenter:

- Dator
  - o Windows PC – Stationär, bärbar
  - o MAC datorer - bärbar
- Mobiltelefon
  - o iOS och Android
- Surfplatta
  - o iOS och Android

Klienttjänsten täcker alla de typer av enheter som användare nyttjar som arbetsredskap, d.v.s. inte bara datorer utan även mobiltelefoner och surfplattor.

Systemen Roomdisplay och PLAYipp administreras av IT-förvaltningen, som sköter all licenshantering. Kostnaden för Roomdisplay täcks av medlemsbidraget, medan verksamheten själv står för kostnaderna för PLAYipp. PLAYipp erbjuder användarna möjlighet att själva styra vilket innehåll som visas på skärmarna.

Denna funktionalitet ingår som standard i klienttjänsten och medlemsbidraget.

GRUNDFUNKTIONALITET	BESKRIVNING
Applikationspaketering	Paketering av programvaror för Windows för distribution via Intune eller SCCM utifrån verksamhetsbehov.
Incidenthantering	Lösning av incidenter. Syftet med en incidenthanteringsprocess är att hantera incidenter för att en verksamhet ska påverkas så lite som möjligt och återställa tjänsten till normalt läge så fort som möjligt.
Problemidentifiering	Problemidentifiering. Syftar till att identifiera och eliminera underliggande orsaker till driftsavbrott och återkommande incidenter.

Service request (tjänsteförfrågan)	En begäran från en användare om en standardiserad tjänst som IT erbjuder. Den skiljer sig från ett incidentärendet genom att det inte handlar om att något inte fungerar, utan snarare att användaren behöver en ny tjänst eller en förändring av en befintlig tjänst.
Konfiguration	Konfiguration av komponenter. Utifrån verksamhetsbehov
Proaktivt underhåll	Uppdatering med firmware och inbyggd mjukvara för att bibehålla funktion och förebygga Incident. Windows Update, drivrutiner och BIOS ingår. Uppdateras automatiskt.
Klientsäkerhet	Tillhandahåller antivirus funktion för datorer, mobiltelefoner och surfplattor
Livscykelhantering av klientkomponenter	<p>Klientkomponenterna som levereras hanteras genom hela livscykeln vilket omfattar följande huvudaktiviteter:</p> <ul style="list-style-type: none"> <li>• <b>Beställning:</b> Hantering av beställning av klienter.</li> <li>• <b>Installation:</b> Installation och konfiguration innan leverans.</li> <li>• <b>Leverans:</b> Beställda och godkända hårdvaror levereras till användarens arbetsplats.</li> <li>• <b>Återlämning och avinstallation:</b> Återlämning av datorer, mobiler och surfplattor hanteras av IT. Skärmar och kring utrustning hanteras av verksamheten.</li> </ul>

## Ansvarsfördelning (vilka komponenter som ingår och vem som är ansvarig)

R =Utförandeansvarig (Responsible). Den part som är ansvarig för arbetet för utförande av aktiviteten.

A = Ytterst ansvarig (Accountable). Den part som är ytterst ansvarig för att aktiviteten utförs korrekt.

C = Konsulteras (Consulted). Resurser vars åsikter är efterfrågade.

I = Informeras (Informed). Ska alltid informeras om status för utförande av aktiviteten.

Innehåll	IT-Nämnd	Kommun/Verksamhet	Kommentar
Incidenthantering	RA	CI	
Problemidentifiering	RA	CI	
Förändringshantering	RA	CI	
Kontinuerlig samverkan med verksamheter diskutera, föreslå och tillhandahålla ett aktuellt grundutbud.	RA	C	
Att grundutbudet är beställningsbart i	RA		

webshop.			
Att tjänsten finns tillgängligt för leverans som motsvarar verksamheternas prognostiserade volym.	RA	C	
Uppdatering av tjänstens operativsystem.	RA		
Bevaka, planera, föreslå och införa uppdateringar och säkerhetsuppdateringar.	RA	CI	
Tillhandahålla programvaror och appar för Windows, Android och iOS	RA	CI	
Verifiering av att klienten är fullt fungerande.	RA		
Tillsammans med verksamheten skapa roadmap för ingående programvaror	RA	C	
Uppdateringar ska genomföras med minimal påverkan för verksamheten och vid större uppdateringar bör användaren via dialogruta kunna styra sin installation	RA	C	
Alla programvaror och operativsystem ska säkerhetsuppdateras regelbundet och enligt överenskommen rutin	RA	C	

## Applikationsdrift

Applikationsdrift innebär övervakning och hantering av applikationer enligt instruktioner fastställda i samråd med systemförvaltare och/eller applikationsleverantör. Den inkluderar övervakning av applikationsspecifika funktioner, analys av incidenter och avvikelser samt hantering av larm och fel för att säkerställa tillgänglighet enligt dokumenterade rutiner.

Drift av applikationer säkerställer tillgängligheten till applikationen. I tjänsten\* ingår att IT-förvaltningen hanterar övervakning, incidenthantering, problemhantering och ändringshantering\*\* av applikationen.

\* IT har inte helhetsansvaret för ett verksamhetssystem. Behov av leverantörsstöd kan förekomma

\*\*vid flytt av databas eller migrering till nya servrar behöver leverantören anlitas

Denna funktionalitet ingår i medlemsbidraget

GRUNDFUNKTIONALITET	BESKRIVNING
Övervakning av applikation	Övervakning av applikation enligt specifikation från applikationsleverantör och verksamhet
Hantering av avvikelser enligt definierade rutiner	Larmhantering Ärenderegistrering Felsökning

	Åtgärdande enligt rutin Kontroll av funktion Återställande av tjänsten
Incidenthantering	Lösning av incidenter. Syftet med en incidenthanteringsprocess är att hantera incidenter för att en verksamhet ska påverkas så lite som möjligt och återställa tjänsten till normalt läge så fort som möjligt. Vid incidenthantering följer IT dom fastställda instruktionerna samt säkerställer att det inte är serverdriften som orsakar incidenten. Beror incidenten på andra faktorer och ifall incidenten är på applikationsnivå, i ett verksamhetssystem, så kontaktar verksamheten leverantören.
Problemidentifiering	Syftar till att identifiera och eliminera underliggande orsaker till driftsavbrott och återkommande incidenter.
Service requests (Tjänsteförfrågan)	En begäran från en användare om en standardiserad tjänst som IT erbjuder. Den skiljer sig från ett incidentärende genom att det inte handlar om att något inte fungerar, utan snarare att användaren behöver en ny tjänst eller en förändring av en befintlig tjänst.
Stopp och start	Stop och start av: <ul style="list-style-type: none"> <li>- specificerade processer och tjänster</li> <li>- applikation inklusive databaser och integrationer</li> <li>- server och infrastrukturkomponenter</li> </ul>
Integration	Övervakning av integration mellan olika system och/eller applikationer via övervakning och larmsättning
Information om larm till avtalade kontakter	Larm eller notifieringar om incidenter, problem eller kritiska händelser skickas till specifika personer eller grupper som har avtalats i förväg. Dessa kontakter kan vara tekniska specialister, applikationsförvaltare, leverantör eller ledning, som ska informeras om och agera på larmet för att hantera situationen snabbt och effektivt.
Upprätthålla driftdokumentation och operativa beskrivningar	Kontinuerlig uppdatering av dokument som beskriver hur applikationer driftas, övervakas och förvaltas.
Rapportering av incidenter	Dokumentation av händelser som påverkar applikationen negativt (exempelvis dess tillgänglighet, säkerhet etc.)
Patchning	Implementering av en mindre uppdatering som korrigerar fel, säkerhetshål eller optimerar prestanda utan att kräva en fullständig ominstallation av applikationen.
Versionsuppgradering	Produktionssättning av betydande nya funktioner eller funktionalitet som inte fanns i den tidigare versionen.

Backup och återställning	Säkerställande av att data kan återställas snabbt efter en incident för att upprätthålla verksamhetens kontinuitet
--------------------------	--

## Ansvarsfördelning (vilka komponenter som ingår och vem som är ansvarig)

R =Utförandeansvarig (Responsible). Den part som är ansvarig för arbetet för utförande av aktiviteten.

A = Ytterst ansvarig (Accountable). Den part som är ytterst ansvarig för att aktiviteten utförs korrekt.

C = Konsulteras (Consulted). Resurser vars åsikter är efterfrågade.

I = Informeras (Informed). Ska alltid informeras om status för utförande av aktiviteten.

Innehåll	IT-Nämnd	Kommun/Verksamhet	Kommentar
Incidenthantering	RA	I	
Tillhandahålla incidentlösningsrutiner	C	RA	
Incidenthantering enligt rutinbeskrivning	R	RA	
Problemidentifiering	RA	CI	
Förändringshantering	RA	CI	
Definiera larmsättning	CI	RA	För applikation och integration
Konfigurera larmsättning.	RA	C	
Justera larmsättning	RA	CI	
Operativ larmhantering	RA		
Applicerings av Patchar	RA	I	Standardpatchar och säkerhetspatchar
Verifieringskriterier av Patchar	C	RA	Standardpatchar och säkerhetspatchar
Verifiering av Patchar	RA	CI	Standardpatchar och säkerhetspatchar
Applicerings av versionsuppgradering	RA	RCI	Större uppdateringar och förändringar.
Verifieringskriterier av versionsuppgradering	C	RA	Större uppdateringar och förändringar
Verifiering av versionsuppgradering	RA	CI	Större uppdateringar och förändringar
Tillhandahålla applikationsspecifika rutiner	C	RA	

## Nätverk

Denna tjänst inkluderar bl.a. övervakning, underhåll och optimering av nätverksinfrastrukturen, inklusive trådbundna och trådlösa nätverk, för att säkerställa hög prestanda, tillgänglighet och säkerhet.

**Nätverksdesign och arkitektur:** Planering och implementering av nätverkslösningar (accesspunkter och switchar) som stödjer verksamhetens behov.

**Övervakning och incidenthantering:** Proaktiv övervakning av nätverkstrafik, bandbreddsanvändning samt identifiering av potentiella problem och snabb åtgärd vid nätverksavbrott.

**Drift och underhåll:** Livscykelhantering av accesspunkter, switchar och brandväggar

**Prestandaoptimering:** Justeringar för att förbättra nätverksprestanda och tillgänglighet.

Denna funktionalitet ingår i medlemsbidraget.

GRUNDFUNKTIONALITET	BESKRIVNING
Internetanslutning	Implementering av ny trådlöst (wifi) eller trådbunden internetanslutning enligt verksamhetsbehov
VPN	För medarbetare och övrigt verksamma, som har behov av att arbeta på distans eller ha tillgång till kommunens resurser under tjänsteresa, finns möjlighet att via VPN ansluta till kommunens nätverk.
Incidenthantering	Lösning av incidenter. Syftet med en incidenthanteringsprocess är att hantera incidenter för att en verksamhet ska påverkas så lite som möjligt och återställa tjänsten till normalt läge så fort som möjligt.
Problemidentifiering	Problemidentifiering på tjänsten. Syftar till att identifiera och eliminera underliggande orsaker till driftsavbrott och återkommande incidenter.
Service request (tjänsteförfrågan)	En begäran från en användare om en standardiserad tjänst som IT erbjuder. Den skiljer sig från ett incidentärende genom att det inte handlar om att något inte fungerar, utan snarare att användaren behöver en ny tjänst eller en förändring av en befintlig tjänst.
Övervakning av nätverkstrafik	<ul style="list-style-type: none"> <li>- <b>Upptäcka säkerhetshot:</b> Identifiering och förebyggning av intrång i realtid.</li> <li>- <b>Optimera prestanda:</b> Upptäcka flaskhalsar och förbättra nätverkets hastighet och tillgänglighet.</li> <li>- <b>Följa efterlevnad:</b> Säkerställa att nätverket uppfyller lagar och regler för datasäkerhet.</li> <li>- <b>Felsökning:</b> Identifiera och lösa nätverksproblem snabbt, vilket minimerar driftstopp.</li> <li>- <b>Kontrollera resurser:</b> Se hur nätverksresurser används och hantera bandbredd för kritiska tjänster.</li> </ul>
Säkerhet	Nätverkssegmentering, implementering av



	brandväggar, säkerhetspatchning, livscykelhantering och andra skyddsåtgärder.
Livscykelhantering av nätverkskomponenter	Kontinuerligt utbyte av accesspunkter och switchar för att säkerställa att nätverket fungerar optimalt samt är säker och pålitlig.

## Datacenter och serverdrift

Datacenter och serverdrift omfattar underhåll, övervakning och hantering av mjuk- och hårdvara.

**Hårdvaruunderhåll:** Installation och hantering av servrar samt lagringssystem.

**Virtualisering:** Hantering av virtualiseringsmiljöer för att optimera resursanvändning och skalbarhet.

**Säkerhet:** Fysisk och digital säkerhet för att skydda datacenter från intrång och störningar.

**Kontinuitetsplanering:** Implementering av redundans, backup och återställningslösningar.

GRUNDFUNKTIONALITET	BESKRIVNING
Backup och återställning	Backup på alla virtuella maskiner och filservrar Backup av databaser och transaktionsloggar Återläsning av säkerhetskopia vid händelse av krasch eller annan förlust av data som påverkar funktionen
Behörighet	Behörighetsadministration av administratörer till operativsystemet
Dokumentation	Upprätthålla dokumentation kring server, operativsystem och infrastruktur. Detta inkluderar ett uppdaterat inventarieregister (CMDB) inklusive licenser för operativsystem
Incidenthantering	Lösning av incidenter. Syftet med en incidenthanteringsprocess är att hantera incidenter för att en verksamhet ska påverkas så lite som möjligt och återställa tjänsten till normalt läge så fort som möjligt.
Lagring	Lagring levereras som en deljänst till fysisk server och virtuell server. Tjänsten bygger på och realiserar av en central plattform för lagring
Serverinstallation	Installation av virtuell standardserver för produktion Skapande av server IP-adressering Installation av supporterat Operativsystem Diskkonfiguration Antivirus Backupagent Övervakningsagent Dokumentation
Service och underhåll	Installation av patchar och servicepacks för operativsystem och infrastruktur sker enligt planering baserat på leverantörernas releasedatum  Uppdatering av firmware och mjukvaror för hårdvara
Säkerhet	Antivirusprogramvara på alla servrar med skydd mot skadlig kod Drift av central antivirusjänst

	Uppdatering av servrar med senaste publicerade definitionsfiler Bevakning av kritiska säkerhetspatchar Installation av brådskande och oplanerade säkerhetspatchar Installation av säkerhetspatchar för operativsystemet, virtualiseringslager och hårdvara
Versionsuppgradering	Produktionssättning av betydande nya funktioner eller funktionalitet som inte fanns i den tidigare versionen.

## Bilaga 4 Termer och förkortningar

TERM ELLER FÖRKORTNING	FÖRKLARING
Accesspunkt	Accesspunkter är nätverkskomponenter som placeras i verksamhetens lokaler för att möjliggöra ett trådlöst nätverk. Utifrån lokalens förutsättningar anpassas antalet accesspunkter
Active Directory (AD)	Katalogtjänst som centralt hanterar användare, datorer, behörigheter och resurser i en organisation.
Applikationsdrift	Applikationsdrift innebär att man tar hand om den applikation en verksamhet väljer att placera på en server. Det innebär löpande drift och underhåll samt övervakningen av en applikation eller mjukvara för att säkerställa att den fungerar som förväntat, är tillgänglig, säker och uppdaterad.
CAB	Change Advisory Board. Möte för att behandla identifierade och nödvändiga ändringar i driftsmiljön.
Change	En change (förändring) är en ändring i en IT-tjänst eller IT-infrastruktur som påverkar hur tjänsten levereras eller fungerar. Målet med en change är att förbättra tjänster, lösa problem, eller implementera nya krav, samtidigt som riskerna för störningar minimeras.
Fastighetsnät	Fastighetsnät är det interna nätet inom en fastighet som sammankopplar fastigheten med avlämningspunkten från fiberleverantören. Avlämningspunkten är vanligtvis placerade i fastighetens källare och via fastighetsnätet kan kunder sedan distribuera olika kommunikationstjänster. Exempel på tjänster som kan distribueras via fastighetsnätet inkluderar internet, telefoni och TV. För att säkerställa en hög kapacitet och hastighet för fastighetens nät är det vanligt att använda fiberkablar.
Incident	Händelse som upplevs som störning eller avbrott i en tjänsts tillgänglighet, säkerhet, prestanda och/eller funktionalitet.
ITIL	Information Technology Infrastructure Library. En samling principer för hantering av IT-tjänster, där fokus ligger på att IT-tjänsterna ska anpassas efter de behov som uppstår i verksamheten.
LAN	Local Area Network. Begränsat nätverk inom kommunernas organisation. Använder fysiska nätverkskablar.
Patch	En uppdatering av programvara som har för avsikt att åtgärda ett fel. En Patch introducerar inte ny funktionalitet till programvaran.
Problem	Process för att finna grundorsak som behöver lösas för att eliminera framtida och upprepade incidenter relaterade till ärendet.
RCA	Root Cause Analysis. Är en metod som används för att identifiera grundorsaken till problem eller incidenter. Målet med RCA är att inte bara åtgärda symtomen på ett problem, utan att gå till botten med vad som faktiskt orsakat det, för att kunna förhindra att det händer igen.
RFC	Request For Change. Är en begäran om en Change.

Serverdrift	Omfattar uppsättning av virtuell server i datacenter. installation av operativsystem, löpande säkerhetskopiering av serverkonfiguration samt uppdaterar och säkerhetshanterar konfigurationen av operativsystemet på din server enligt regelbundna intervaller.
Service request (Tjänsteförfrågan)	En service request (tjänsteförfrågan) är en formell begäran från en användare för att få en specifik tjänst eller åtgärd utförd av en IT-avdelning eller annan serviceleverantör. Det kan handla om allt från att få tillgång till system, beställa ny utrustning, eller be om hjälp med att återställa sitt lösenord ifall man har glömt det.
SMTP	Simple Mail Transfer Protocol. Kommunikationsprotokoll för att leverera elektronisk post.
Standard Change	Standard Change enligt ITILs definition. Standard Change är fördefinierad, spåras ej med RFC och behandlas inte i CAB.
Swicth	En switch är en nätverkskomponent som används för att koppla ihop enheter, såsom datorer, servrar och skrivare, inom ett lokalt nätverk (LAN).
Verksamhetssystem	System/applikation som används av verksamheten, som ex ekonomisystem, intranät, vårdssystem etc
Versionsuppgradering	Versionsuppgradering är processen där en applikation, ett system eller en programvara uppdateras till en nyare version. Detta skiljer sig från en vanlig patch eller mindre uppdatering eftersom en versionsuppgradering ofta innebär större förändringar, nya funktioner och förbättringar, samt ibland omfattande förändringar i gränssnitt eller arkitektur.
UPS (Uninterruptible Power Supply)	Avbrottsfri kraftkälla med batteri som ger reservström vid elavbrott
VPN (Virtual Private Network)	En VPN är en teknik som skapar en säker, krypterad anslutning över internet mellan en användares enhet och kommunens nätverk. Det används av organisationer för att skydda data, särskilt när anställda arbetar på distans, genom att säkerställa att känslig information inte kan avlyssnas eller stjälas under överföringen
WAN	Wide Area Network är ett datornätverk som sträcker sig över ett stort geografiskt område, ofta mellan städer, länder eller kontinenter. Till skillnad från lokala nätverk (LAN) som täcker ett begränsat område som ett kontor eller hem, kan ett WAN förbinda datorer och nätverk på långa avstånd. Exempelvis ett företagsnätverk som sammanbinder kontor på olika platser
WLAN	Wireless Local Area Network. Trådlöst LAN. Ett lokalt nätverk som använder trådlös (wifi) teknik för att ansluta enheter. Det tillåter datorer, mobiltelefoner, och andra enheter att kommunicera och dela internetanslutning utan fysiska nätverkskablar.