

# Service Level Agreement mall för kommunalt IT-stöd

v1.0 - 2010-11-02

**Kim Weyns & Martin Höst**  
**Institutionen för Datavetenskap, Lunds Universitet**  
**Box 118, S-221 00 Lund**  
**kim.weyns@cs.lth.se**

## Inledning

Ett Service Level Agreement (SLA) är en överenskommelse mellan en IT-leverantör och en kund. Den beskriver detaljerna på tjänsterna som leverantören levererar till kunden. På senare tid, bland annat genom det ökade intresset för ITIL, har det blivit vanligare att också använda SLA-avtal internt i en organisation för att beskriva relationen mellan organisationens IT-enhet och resten av verksamheten.

En nyligen utförd studie har visat att många kommuner i Sverige har börjat använda sig av SLA-avtal i sin verksamhet. Studien visar också att det ofta är svårt att skriva effektiva SLA-avtal och att inte alla möjligheter som ett bra SLA erbjuder utnyttjas i praktiken. IT-stöd i en kommun skiljer sig också från IT-stöd i ett privat företag och därför behöver SLA-tekniken anpassas för att vara användbar på kommunal nivå.

Ett SLA kan användas som kontrakt eller som prisöverenskommelse mellan två parter, men ännu viktigare som kommunikationsplattform för viktiga frågor kring informationssäkerhet. Det är den senare delen som denna SLA-mall fokuserar på.

Denna mall består av ett ramverk med de olika delar som ett bra SLA bör innehålla. SLA-mallen kan användas som checklista för att uppdatera befintliga SLA och mallens struktur kan också användas som grundstruktur för att skriva nya SLA-avtal.

SLA-mallen är ganska omfattande och inte alla element i mallen är nödvändigt i varje SLA. Mindre organisationer eller organisationer som just börjat använda sig av SLA-avtal kan börja i en mindre skala genom att först välja ut de viktigaste delarna av mallen för en första version och sedan lägga till mer detaljer när SLA-tekniken är mer inarbetad i organisationen.

Det finns flera olika sätt att skriva SLA-avtal inom en organisation. Det mest grundläggande sättet är att ha ett SLA som gäller för hela organisationens verksamhet. För att hantera de stora skillnaderna mellan IT-behov av olika förvaltningar kan man också ha ett SLA för varje förvaltning eller organisatorisk enhet. Det mest avancerade sätt att använda SLA är att ha ett separat SLA för varje system, vilket gör det lättare att också fånga specifika behov som finns för vissa system. De flesta delarna i mallen är tillräckligt generella för att vara användbar i alla tre fallen, men strukturen kan behöva anpassas om ett SLA skrivs för varje system. Mallen är också

användbar både för verksamhetsspecifika system som ägs av verksamheten och för system som ägs av IT-enheten.

Det viktigaste med att skriva ett SLA är att det blir ett praktiskt användbart dokument för både IT-enheten och verksamheten. Kundperspektivet och verksamhetsnyttan måste vara utgångspunkten för tjänstenivåer som beskrivs i ett SLA-avtal. Ett SLA ska vara ett levande dokument som ses över regelbundet och som uppdateras när IT-systemen eller verksamhetens användning av de systemen ändras.

Målgruppen för denna SLA-mall är främst svenska kommuner och myndigheter med en relativt liten IT-enhet men med flera samhällskritiska IT-system med höga krav på informationssäkerhet.

Denna SLA-mall är baserad på en studie av hur SLA-avtal används på Svenska kommuner, samt på ett antal publik tillgängliga internationella SLA-mallar och tidigare forskning publicerad om SLA.

Mallen är framtagen inom FRIVA-projektet ( <http://www.friva.lucram.lu.se/> ) som finansieras av MSB, Myndigheten för Samhällsskydd och Beredskap.

# Service Level Agreement

## 1. Mål

Måldelen introducerar och definierar båda parter som ingår i detta SLA och beskriver tydligt organisationens mål med skrivandet av SLA-avtalet. Målen borde representera båda kundens och leverantörens mål, baserad på organisationens gemensamma övergripande mål. Verksamhetsnyttan borde stå central i organisationens IT-stöd och det borde tydligt framgå från SLA-avtalet.

Målen kan till exempel innehålla:

- Att definiera de tjänstenivåer som gäller för alla system
- Att tydliggöra ansvarsfördelningen mellan parterna
- Att tydliggöra och definiera avgränsningar för IT-stöd
- Att definiera systemägare och systemförvaltare för alla system
- Att uppnå ett mer standardiserat IT-stöd inom organisationen
- Att definiera informationsvägar inom organisationen gällande informationssäkerhet
- Budgetavtal mellan parterna
- Att sätta förväntningar rätt mellan parterna för att undvika konflikter
- Att förtydliga relationen mellan verksamheten, IT-enheten och externa leverantörer

## 2. Avgränsning

Detta stycke beskriver vilka tjänster som är inkluderade i SLA-avtalet, och vilka IT-tjänster som explicit inte är del av avtalet. Här ges också en översikt av de viktigaste ansvarsområdena av båda parter. Alla processer som följer i resten av dokumentet borde finnas i minst en av båda listerna.

### IT-enheten ansvarar för:

(med explicita hänvisningar till respektive del av SLA-avtalet)

### Förvaltningarna ansvarar för:

(med explicita hänvisningar till respektive del av SLA-avtalet)

## 3. Tjänstenivåer

Detta stycke är huvuddelen av SLA-avtalet som definierar vilka tjänstenivåer som gäller för olika system och tjänster. En kommun, eller en annan organisation med ett viktigt samhällsansvar och en aktiv roll i krishantering, har ett behov av IT-stöd utöver vanlig arbetstid. Samtidigt finns det också många system som inte behöver prioriterat IT-stöd. Därför är det logiskt att definiera minst två tjänstenivåer: en grundnivå och en mer prioriterad nivå för de mest kritiska systemen. SLA-avtalet ska då innehålla en explicit lista med alla kritiska system som behöver en högre nivå av IT-stöd. För vissa system som bara är kritiska under vissa speciella omständigheter kan man definiera undantag från grundnivån (till exempel för lönesystemet på de dagarna varje månad som lönerna ska utbetalas).

För de flesta system som inkluderas i grundnivån räcker det att definiera tjänstenivån för tillgänglighet, IT-support och säkerhetskopiering. För de mest kritiska system behöver man ytterligare definiera prestandakrav (t.ex. för det interna nätverket, för telefonisystemet eller för

organisationens publika hemsida) och IT-säkerhetskrav (för system som innehåller sekretessbelagd data).

### Tillgänglighetskrav

Tillgänglighetsmål för alla system i grundnivån ska definieras, till exempel 99% som överensstämmer med en nertid av mindre än 90 timmar om året. Det borde ta hänsyn till både planerade och oplanerade driftstop.

En viktig faktor för tillgängligheten är tillgången till reservkraft. Det kan vara bra att explicit ange i SLA-avtalet vilka system som ska vara anslutna till reservkraft, till exempel baserat på en scenarioanalys om ett längre strömavbrott i kommunen.

### IT-supportprocesser

IT-support är ofta en av de mest grundläggande faktorerna som definieras i ett SLA, och det finns flera delar som definieras i ett bra SLA, t ex:

- Öppettider, vardagar och helgdagar, båda för kritiska system och icke-kritiska system.
- Max-/genomsnittssvarstider
- Mål för lösningstider
- 'Nöjd-kund-index': andel av supportärenden som löses på ett tillfredställande sätt
- Uppföljning: hur kunden informeras om lösandet av ärenden
- Prioritering av ärenden
- Krav på verksamheten att vara kontaktbar medan högprioriterade problem löses
- Regelbunden tillgång till en IT-tekniker på plats på varje avdelning för att diskutera och lösa mindre problem
- Utbildning till användare

### Säkerhetskopiering

En annan viktig process som borde definieras i varje SLA handlar om rutinerna för säkerhetskopiering. Det är viktigt för användare att veta vilka möjligheter och begränsningar som finns för att återskapa data från säkerhetskopior.

Det viktigaste attributet att definiera för säkerhetskopiering är frekvensen, både för inkrementell och total säkerhetskopiering. Men det är också viktigt att explicit ange i SLA-avtalet hur lång tid det förväntas ta att återskapa de mest kritiska system från säkerhetskopian.

## 4. Risk- och sårbarhetsanalyser

Alla systemägare för kritiska system borde vara ansvariga att utföra risk- och sårbarhetsanalyser för dessa system. IT-personal borde aktivt medverka i dessa analyser.

## 5. Incidenthantering

Incidenthantering är en del av supportprocessen, men hanteringen av de mest kritiska supportärendena är tillräckligt viktig att diskuteras separat i ett SLA-avtal. För alla incidenter med kritiska system ska det finnas en formel incidenthanteringsprocess. Processen borde inkludera de mest brådskande åtgärder men också uppföljningen av lärdomar från incidenten för att motverka att liknande incidenter inträffar för samma eller andra system.

För större IT-incidenter borde en incidentgrupp sammankallas. Då ska all nödvändigt personal finnas till hands för att lösa problemen och för att samtidigt hålla användare informerad om problemet, samt om hur länge det kan tänkas pågå.

Även för andra krissituationer som inte är direkt IT-relaterade, kan organisationen behöva sammankalla en krisledningsgrupp. Denna krisledningsgrupp kommer antagligen att vara beroende av ett antal kritiska IT-system i krisledningscentralen. Också rutiner för att säkra tillgången till supporten för dessa IT-system borde ingå i SLA-avtalet och i organisationens krisplaner.

## 6. Innovationsprocesser

Informations- och kommunikationstekniken kännetecknas av en mycket snabb utveckling, och ett bra SLA borde definiera ansvarsområden för att introducera nya system eller uppdateringar av befintliga system inom organisationen. Till exempel:

- Rutiner för att beställa och installera ny mjukvara
- Rutiner för att beställa ny hårdvara
- IT-projekt för beställning och genomförande av större innovationer inom organisationens IT-system.
- Rutiner för mjukvaruuppdateringar
- Möjligheter att testa nya applikationer inom en testmiljö

## 7. Relaterade dokument

Om organisationen använder sig av några av följande dokument, borde de nämnas i SLA-avtalet och ansvarsfördelningen för dessa dokument borde definieras, samt hur de påverkar informationssäkerheten:

- Informationssäkerhetspolicy
- Användarriktlinjer
- Användarhandbok
- Systemdokumentation
- Kontrakt med externa leverantörer
- Regler för sekretess
- Regler för offentlighetsprincipen
- Nationella eller internationella standarder, t ex BITS, ITIL, ...

## 8. Uppföljning

Det är också viktigt att följa upp att IT-supporten också uppfyller de utlovade tjänstenivåer som definierats i SLA-avtalet. Dessa nivåer kan bara kontrolleras om de skrivits på ett mätbart sätt och också mäts kontinuerligt. Att definiera en mättningsplan tillsammans med SLA-avtalet är ett bra sätt att se till att SLA-avtalet skrivits på ett mätbart sätt och inte på en för abstrakt nivå. Att mäta de viktigaste utfallen av IT-supporten underlättar också för organisationen att detektera möjliga informationssäkerhetsproblem så tidigt som möjligt.

Denna mätplan bör inte bara beskriva hur informationssäkerheten ska mätas utan också hur den insamlade datan ska analyseras och rapporteras till alla inblandade.

Den snabba IT-utvecklingen betyder också att SLA-avtalet antagligen kommer att behöva uppdateras regelbundet. Denna del av SLA-avtalet bör också definiera hur ofta dokumentet kommer att ses över och uppdateras vid behov. Den insamlade datan från mätningarna kan också visa på vilka tjänstenivåer i SLA-avtalet som bör ses över.

SLA-avtalet bör också definiera ansvarsfördelningen för att sprida informationen om SLA-avtalet och eventuella ändringar i avtalet till alla berörda verksamheter. Den senaste versionen av SLA-avtalet bör vara tillgänglig för alla användare och för IT-personalen. Systemägare bör se till att alla användare är medvetna om de viktigaste bestämmelserna och begränsningarna i SLA-avtalet, samtidigt som IT-chefen ser till att IT-personalen är medveten om SLA-avtalet.

## 9. Finansiella aspekter

Beroende på den interna strukturen av organisationen, kan SLA-avtalet också användas för att hantera en del praktiska och finansiella aspekter mellan IT-enheten och resten av organisationen. I många SLA-avtal har dessa frågor blivit huvuddelen i dokumentet, men i ett komplett SLA ska huvudfokus ligga på att definiera tjänstenivåer och inte på dessa finansiella aspekter.

Dessa finansiella aspekter kan till exempel vara:

- Prisöverenskommelser för tjänsterna levererade av IT-enheten
- Hantering av mjukvarulicenser
- Försäkringar för hårdvara inkluderat i överenskommelsen
- Möjlig kompensation när IT-supporten inte uppfyller de lovade tjänstenivåer. Finansiell kompensation är ofta inte meningsfull internt inom en organisation, däremot kan det vara bra att ställa krav på en explicit utredning eller rapport från IT-enheten om IT-enheten inte uppfyller de ställda kraven på samma sätt som efter större incidenter.

## 10. Bilagor

SLA-avtalet ska helst också innehålla följande bilagor:

- Ordlista
- Lista som definierar systemägare och systemförvaltare för alla system
- Kontaktlista för alla ärenden inkluderade i SLA-avtalet, både hos verksamheten och hos IT-enheten
- Klassificering av alla kritiska system gällande konfidentialitet, riktighet och tillgänglighet, baserad på MSB:s klassificeringssystem.
- Beskrivning av kritiska beroende mellan system