TIMRÅ KOMMUN
Kommunledningskontoret

Vägledande råd och bestämmelser – Förvaltning & Drift av IT inom Timrå kommun (Q4 2018)

System eller Applikation?

Med systemförvaltning avses förvaltning av allt IT-stöd som används inom kommunen. IT-stöd kan uppdelas i IT-system och applikationer. Definitionen för uppdelningen IT-system och applikation är:
*Med **IT-system** avses ett IT-stöd som samlar in, lagrar, bearbetar och distribuerar information och därigenom stödjer kommunikation och arbete inom och mellan organisationer. Övrig programvara definieras därmed som **applikationer**.*

Syftet med systemförvaltning är att ge möjlighet till planering och utveckling av IT-stödet utifrån ekonomi, säkerhet, verksamhetsnytta och arbetsmiljö.

Definition av system

Vad är ett system? För att klargöra för vilka system som detta gäller, så har vi delat in dem i tre olika klasser. Definitionen av kommunens alla system finns också hos informationssäkerhetssamordnaren.

Stor – Kommunens 10 prioriterade system. Här gäller samtliga riktlinjer.

Mellan – 25-150 användare, egen server

Liten – Färre än 25 användare och ligger på en gemensam applikationsserver

Organisation och ansvar

Systemförvaltning omfattar många roller. Verksamheten har sina roller kring systemförvaltningen. Hos driftleverantören finns roller som inte kommer att beskrivas i detta dokument. Anledningen är att rollerna kan skilja sig mellan olika driftleverantörer. Därutöver kan det även finnas en systemleverantör, som är den organisation som tillverkar/sålt IT-stödet.

Förvaltnings- eller Enhetschef är systemägare och ansvarig för IT-system som stödjer den egna verksamheten. Systemägare för teknisk infrastruktur är IT-chefen.

Ansvarsfördelningen ska medverka till att stödja verksamheten och uppfylla informationssäkerhetens mål. Detta innebär att ett IT-system, med alla dess delar, är en resurs i en verksamhet på samma sätt som personal och lokaler.

Det övergripande ansvaret för kommunens IT-system har kommunstyrelsen.

Postadress: 861 82 Timrå
Besöksadress: Köpmangatan 14
Telefon: 060-16 31 00
Bankgiro: 5672-9387
Organisationsnummer: 212000-2395
Fax: 060-16 31 05
Hemsida: www.timra.se
E-post: info@timra.se

Säkerhet

Ett IT-system behandlar väldigt ofta personuppgifter. Enligt dataskyddsförordningen är verksamhetens nämnd ansvarig för denna behandling och därmed ansvarig för att säkerställa att den är korrekt och säker. Det är därför viktigt att verksamheten säkerställer ett korrekt skydd för IT-systemet och att rätt personer har behörigheter till det.

En viktig del i att säkerställa ett adekvat skydd av personuppgifterna är att löpande uppdatera till nya versioner och underhålla IT-systemet. Kom ihåg att servicedesk aldrig uppdaterar ett system utan en beställning från systemförvaltaren av systemet. Förvaltaren måste ha en löpande dialog med den avtalade leverantören av systemet för att planera in och beställa uppdateringar. Samma gäller att man via behörighetsstyrning tillåter rätt personer att ha tillgång till uppgifterna i systemet. Det är även viktigt att ha detaljkoll på vilka personuppgiftsbehandlingar som sker i systemet. Detta ska också dokumenteras i registerplanen för GDPR. Det är normalt systemförvaltaren av IT-systemet som har en överblick över samtliga behandlingar som sker i systemet och även högre administratörsrättigheter.

Verksamhetsnytta

Kanske det viktigaste i slutändan med att förvalta ett system, är att säkerställa verksamhetsnyttan. IT-system kan lätt bli snarare ett hinder än ett stöd i en verksamhet om det inte förvaltas korrekt. Det kan också bli så att man inte använder det i den utsträckningen man har tänkt eftersom man inte har möjlighet till support eller kompetents för att använda det. I systemförvaltningen ingår det att säkerställa att IT-systemet stöttar verksamhetens processer på bästa möjliga sätt och agera kravställare mot avtalad leverantör och servicedesk om IT-stödet inte stöttar verksamheten på bästa sätt.

Arbetsmiljö

Ett väl fungerande IT-stöd förenklar medarbetarens vardag. Ett dåligt fungerande system kan istället tvärtom försvåra en medarbetares vardag och bli ett arbetsmiljöproblem. Ett krånglande och icke användarvänligt IT-stöd är en tidstjuv och ett irritationsmoment i det dagliga arbetet. Därför är det viktigt att löpande säkerställa att drift och supportrutiner fungerar samt att verksamhetens krav och synpunkter beaktas i utvecklingen av IT-stödet.

IT-Forum

IT-forum består av förvaltningschefer, systemförvaltare och IT-enheten. Uppgifter;

- strategi utifrån verksamheternas behov av IT-stöd efter underlag från systemförvaltarna
- strategi för IT-säkerhetsarbetet och kommunens säkerhetsinstruktioner

efter underlag från IT-säkerhetssamordnaren
- beslut av sekretessförbindelser/personuppgiftsbiträdesavtal för konsulter och serviceföretag efter underlag från GDPR-samordnarna, systemförvaltare

Systemägare

Systemägare måste finnas för alla IT-system. Dock så gäller flera av nedanstående endast för mellan och stora system. Systemägaren har ansvar för:

- Att för varje system utse två systemförvaltare med den kunskap som krävs för respektive system. För system ”liten” räcker det med en systemadministratör
- Att inför verksamhetsplaneringen initiera och föreslå den egna verksamhetens behov av IT-stöd till IT-forumet
- Att externa leverantörer av tjänster och produkter blir informerade om kommunens informations- och säkerhetskrav
- Att i en riskanalys fastställa eventuella krav. Denna ska också kontrolleras årligen samt uppdateras vart tredje år, eller vid nyinköp av nytt system (stor och mellan)
- Att organisation och befattningar som rör systemet möter aktuella behov
- Att fastställa IT-systemets dokumentation och användarhandledning
- Att årligen rapportera till IT-enheten om interna kontroller som genomförts vid förvaltningen under det senaste året, och vilka som planeras till nästkommande år
- Att fatta beslut om utveckling av IT-systemet vad gäller nya funktioner och samverka med IT-enheten
- Ansvarar för att IT-stödet följer lagar, förordningar och interna styrdokument
- Att licenser och avtal finns enligt krav
- Att initiera ny upphandling vid utgång av leverantörsavtalet till upphandlingsenheten
- Att i samverkan med IT-chef fastställa kontinuitetsplan för verksamhetssystemen (stor och mellan)
- Att driftgodkänna verksamhetssystemet

IT-säkerhetsutbildning

Systemägare ansvarar för
- att de egna medarbetarna erhåller information och utbildning om innehållet i de riktlinjer (VROB) de är berörda av
- att medarbetare, före tilldelning av behörighet, har tillräckliga kunskaper om säkerhetsreglerna för de IT-system de behöver för de egna arbetsuppgifterna, genom utbildning och VROB (Vägledande Råd Och Bestämmelser).

Varje enskild medarbetare har ett ansvar att påtala det egna behovet av utbildning.

Distansarbete

Systemägaren och verksamhetsansvarig chef ska besluta om ett IT-systems information ska få hanteras på distans med stationär eller mobil utrustning.

Loggning och spårbarhet

Målet är att det i samtliga IT-system ska finnas en säkerhetslogg, som registrerar användaridentitet, uppgift om inloggning och utloggning samt datum och klockslag. Systemägarnas övriga krav på säkerhets- och transaktionsloggar ska framgå av de säkerhetsplaner som respektive systemägare upprättat.

Säkerhetskopiering och lagring

Systemägarnas krav på säkerhetskopiering och lagring för de egna systemen ska framgå av de riskanalyser som respektive systemägare upprättat. Kraven i dessa planer ska vara koordinerade i analyser för teknisk infrastruktur.

Följande är kommunens basrutiner gällande backup:

- Backup tas varje natt mellan 22:00 -06:00
- Kopia i annan byggnad
- Antal versioner: 7 st

Backup och restora av förlorat data, som ligger inom ovanstående regler hanteras av EVRY one Outsourcing Services Malmö

Driftgodkännande av mjukvara

Systemägaren skall driftgodkänna mjukvaran innan den driftsätts. Driftgodkännandet skall bland annat innefatta driftstester, säkerhetstester och uppföljningar av eventuella ändringar sedan tidigare versioner. Beroenden med andra mjukvaror skall dokumenteras tillsammans med hur mjukvaran är installerad, hur den körs och av vem den körs i driftdokumentationen. Vid nyinköpt mjukvara ska det alltid föregås av en verksamhets/riskanalys.

Systemförvaltare

Systemförvaltare utses av systemägaren och ska vara två till antalet för varje system som betecknas som stort eller mellan. Det är de personer som har ansvaret för den dagliga användningen av IT-systemet.

Systemförvaltarna ansvarar för systemförvaltning utifrån systemägarens direktiv, vad gäller tillämpning i verksamheten, användarnas krav och behov samt att förväntade nyttoeffekter realiseras. De ska även medverka i arbetet med framtagande av en riskanalys.

Systemförvaltarna skall ha en djup kunskap om den verksamhet som systemet ska

stödja samt övergripande kunskap om tekniken som tillämpas i systemet. Vidare skall systemförvaltarna säkra att det finns en fungerande förvaltnings- och utvecklingsmodell, där alla ingående parter samverkar kring systemets användning och utveckling.

Parterna är primärt systemägare, administratörer, användargrupper, applikationsleverantör och driftleverantör.

Organisation
Systemförvaltarna rapporter till systemägaren. Systemförvaltarna driver sina egna forum för att säkerställa att systemet används och utvecklas på det sätt som bäst gynnar verksamheten. Systemförvaltarna tillhör både kommunens systemförvaltargrupp och förvaltningens systemförvaltargrupp.

Arbetsuppgifter

- säkerställa att det finns ett systemägardirektiv
- säkerställa att det finns en förvaltningsplan inkl. budget för ingående verksamhetsår
- säkerställa att det finns en 2-årig utvecklingsplan inkl. budget
- hålla regelbundna möten med systemets administratörer och användare för att få kunskap om hur systemet fungerar i verksamheten.
- se till att systemdokumentation och media finns tillgängliga och är uppdaterade
- se till att användarhandböcker finns tillgängliga och är uppdaterade
- säkerställa utbildning och att systemet används på rätt sätt i verksamheten
- hantera eventuella behörigheter till systemet (framförallt hantera behörigheter för systemadministratörer)
- se till att avtal finns med applikationsleverantör avseende support och nya releaser
- se till att personuppgiftsbiträdesavtal finns skrivet om systemet behandlar personuppgifter
- se till att avtal finns med driftleverantör avseende drift av applikationen
- säkerställa att avtalen mellan applikationsleverantör och driftleverantör hänger ihop
- genomföra kontinuerliga avstämningar med applikations- och driftsleverantör där planer och behov diskuteras.
- fånga upp problem, rapportera och driva dessa gentemot applikationsleverantör och driftleverantör
- koordinera och testa nya releaser av systemet
- se till att riskanalys genomförs och följs upp vart tredje år.

Systemadministratör

Systemadministratören innehar den tekniska kompetensen och ansvarar tillsammans med systemägaren och systemförvaltaren för att den dagliga driften upprätthålls enligt överenskommelse. Denna roll kan även vara samma person som

Systemförvaltaren på stora och mellan system, om så systemägaren anser det lämpligt. Systemadministratören ansvarar för att:

- Support till användarna i verksamheten
- Administrera behörigheter och lösenord
- Delta i och stödja IT-säkerhetsarbetet
- Initiera felsökning vid driftsstörningar/avbrott och vidta nödvändiga åtgärder och rapportera till Systemförvaltaren/Ägaren
- Lämna förslag på förändringar
- Medverka vid framtagning av kostnads och lösningsförslag
- Upprätthålla avtalad kvalitet på systemet

Behörighetsadministration

Det är nödvändigt att administration av och regler för behörighetstilldelning är klart fastlagda och kända. Detta innebär att;

- behörigheter ska alltid beställas av en ***Behörig beställare*** som är utsedd av förvaltningschefen
- endast behörig användare anställd i kommunen, ges åtkomst till kommunens IT-system. Undantagsfall kan behörighet ges tillfälligt till leverantörer
- användares behörighet ska styras utifrån dennas arbetsuppgifter och efter beslut av chefen
- varje användare ska ha en personlig identitet bestående av login-id och lösenord. Lösenord ska bytas vid uppmaning efter 180 dagar.
- den som är tjänstledig eller av annan orsak har längre frånvaro skall ha sin identitet spärrad
- uppföljning och revidering av tilldelade behörigheter ska ske regelbundet av respektive systemförvaltare.

Krav för hur behörigheter ska hanteras ska finnas i riskanalysen för respektive system. Dessa skall även beskriva vem som ansvarar för att systemen justeras för att motsvara önskad policy, vem som ansvarar för att behörigheter godkänns samt vem som ansvarar för att behörigheterna läggs upp, hanteras och revideras.

För lösenord bör det framgå hur lösenordet ska vara beskaffade i form av längd och komplexitet men även hur byte av lösenord får ske. Externa konsulter, vikarier och projektanställda ska alltid ha tidsbegränsning på sina konton.

Användarna ska endast ges behörighet till det som är relevant för deras arbetsuppgifter. Avvikelse från detta skall loggas.

Avvecklingsfasen

IT-stöd avvecklas oftast p.g.a. att det ska ersättas med ett annat. När ett IT-system avvecklas måste man ställa sig frågan hur man hanterar den information som finns i

IT-systemet. Systemägaren ska, i samråd med arkivarie, besluta i vilken grad informationen ska föras över till det nya IT-systemet och i vilken grad informationen ska arkiveras. Beslutet ska dokumenteras. IT-stöd har ofta integrationer och beroenden till andra IT-stöd. Vid avveckling måste kopplingar till, och konsekvenser för, andra IT-stöd utredas. När ett IT-stöd har beslutats att avvecklas ska en plan tas fram.

IT-chef

IT-chef är systemägare för den tekniska infrastrukturen och har det övergripande ansvaret för att de kommungemensamma systemen tekniskt fungerar.

IT-chefen ansvarar också för IT-forumets funktion upprätthålls och att samtliga mål och planer tas fram.

Tillträdesskydd

IT-chef ska besluta om vilka som ska ha tillträde till kommunens datahall.

IT-säkerhets & Informationssäkerhetssamordnare

IT-säkerhetssamordnaren stödjer arbetet med att uppnå informationssäkerhetspolicyns mål. Detta kan innebära utvärdering samt deltagande i diskussioner kring metoder, plattformar och IT-system, delta i interna och externa kontaktnät,. IT-säkerhetssamordnaren är ett stöd för verksamheterna och är i IT-säkerhetsfrågor direkt underställd kommunchefen.

IT-säkerhetssamordnaren ska stödja systemägarna i arbetet med att ta fram Risk och sårbarhetsanalyser. Samordnaren ska även se till att informationsklassningen, lagar ska vara väl kända inom kommunen. Även den interna kontrollen av att verksamheterna följer lagar och bestämmelser ansvarar IT-säkerhetssamordnaren för. Denne ska informera IT-chefen löpande.
Ytterst ansvarig för kommunens IT-säkerhet är kommunchefen.

IT-incidenthantering

IT-säkerhetssamordnaren ska sammanställa och rapportera till ledningen. Detta redovisas årligen i ett bokslut från IT-enheten;

- intrång och försök till intrång
- brott mot lagstiftning och interna regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar.

- Alla kritiska händelser rapporteras från Evry outsoursing
- Rapportering av virus och skadlig kod i Timrås IT-miljö till IT-samordnare på Timrå

IT-säkerhetsarbete

Krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en *Verksamhets/riskanalys*. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten, kommunens 10 prioriterade. Dessa analyser ska sedan kontrolleras varje år och uppdateras vart tredje år.

Mjukvara

Definition mjukvara; programvara (applikationer, operativsystem etc.) som installeras på klienter, servrar samt programvara (firmware, bios etc) som installeras i enheter som är framtagna för endast ett syfte såsom brandväggar, switchar och routrar.

Installation

Installationsproceduren ska dokumenteras i detalj för att minimera risken för att installationerna skiljer sig åt. Förändringar i mjukvaran ska hanteras som ett nytt distributionspaket. Installation bör först ske i begränsat omfång för att göra ett säkerställande av installationen och först därefter slutförs installationen på resterande enheter.

Systemägaren ansvarar för att utvärdera installationen innan den driftgodkänns. Då systemägaren anser att mjukvaran uppfyller driftgodkännandet kan installationen slutföras. Som regel skall uppdateringar aldrig ske automatisk utan att först acceptanstestas.

Hårdvara

Utrustning (datorer, skärmar, switchar etc.) som installeras i kommunens produktionsmiljö ska standardiseras för att minimera support och problem.

Systemägaren skall efter samråd med driftpersonal driftgodkänna hårdvaran innan den driftsätts. Installationsproceduren skall dokumenteras för att minimera riskerna för att installationerna skiljer sig åt.

Antivirusprogram

Antivirusprogrammet på klienter och servrar ska uppdateras automatiskt. Brandväggen hanterar kopplingen mellan näten internt, mot Internet samt mot externa leverantörer.

Reservkraft

Det finns reservkraft i form av UPS:er, och ett centralt dieselaggregat vid kommunhuset som automatstartar vid strömbortfall.

Loggning & spårbarhet

Krav för hur loggning ska ske, ska finns dokumenterat i riskanalysen för respektive system. Dessa skall även beskriva vem som ansvarar för att systemen ställs in till önskad loggningsnivå, vem som ansvarar för att loggarna förvaras, hanteras och analyseras samt vem som får begära ut loggar.

Vanligtvis loggas in-, utloggningar samt försök till dessa, förändringar i systeminställningar, omstarter osv. Det är upp till systemägaren att ställa krav på vad systemet skall logga och hur länge loggarna skall sparas. Systemägaren kan i vissa fall ställa krav på att analys/automatisk analys av loggarna skall ske regelbundet.

Vid misstanke om intrång/obehörig access eller systemfel överlämnas analysunderlaget till IT-enheten och systemägaren för beslut om vidare åtgärd.

Kommunikation

IT-enheten ansvarar för att systemen ställs in till önskad policynivå och godkänner kommunikationsförändringar samt ansvarar för att denna kontrolleras och revideras.

Om det finns användare som använder sig av fjärraccess i någon form behöver dessa hanteras på ett speciellt sätt.

Kommunikation med t.ex externa leverantörer och Internet skall vara hårt reglerad och finnas väldokumenterad så att felsökning och prestandaproblem kan lokaliseras lättare.

Övervakning

Krav för vad som skall övervakas, hur och när och vilka åtgärder som ska vidtas vid driftslarm skall finnas dokumenterade. Systemägaren skall ställa krav på ovan nämnda uppgifter i enlighet med det tillgänglighetskrav som satts på systemet.

Övervakning av prestanda bör ske mot samtliga verksamhetskritiska system. Vid överlast på dessa larmas driftansvarig via övervakningssystemet.

Tillgänglighet

Tillgängligheten för samtliga system skall regelbundet följas upp av driften och IT-enheten. Avvikelser ska rapporteras och åtgärdas.

Administration

För att underlätta administrationen är det viktigt att likformighet gäller genomgående för samtliga system, t.ex. namngivning av hårdvara etc. Vidare skall journalföring, bemanning, kompetenskrav och eventuella ersättare definieras per system

Servicefönster

Krav för när systemunderhåll kan ske på systemen skall finnas. Dessa skall ange när underhåll kan göras, vilka system som påverkas samt vem som kan göra acceptanstest efter utfört underhåll om så krävs. Systemunderhåll bör göras vid ett servicefönster.

Incidenthanteringsprocessen

- Genomgång av loggar samt oväntade händelser i systemen.
- Säkring av data, spårande av källa och säkrande av eventuellt bevismaterial. Förebyggande åtgärder för att motverka liknande.
- Slutsats och dokumentation av händelsen.
- Eventuell polisanmälan.

TIMRÅ KOMMUN
Kommunledningskontoret

Bilaga 1

1 Inledning

Denna systemförvaltningsplan finns kommunicerad via TimNet

1.1 Beskrivning av IT-stödet och nyttan

1.2 Systemförvaltningens omfattning

1.3 Personuppgifter

Innehåller systemet personuppgifter?	☐ JA ☐ NEJ

Om systemet innehåller personuppgifter:

Är personuppgiftsbehandlingarna dokumenterade i det gemensamma registret?	☐ JA ☐ NEJ

1.4 Informationssäkerhetsklassning

Information	Konfidentialitet	Tillgänglighet	Riktighet	Spårbarhet

1.5 Kontinuitetsplan

Finns en kontinuitetsplan för verksamheten?	☐ JA ☐ NEJ

1.6 Informationens bevarande

Informationshanteringsplan / dokumenthanteringsplan	Kontaktperson i verksamheten

1.7 Avtal och SLA

Typ av avtal	Motpart	From datum	Tom datum	Kommentar
SLA				
Personuppgifts-biträdeseavtal				

1.8 Historik

Datum	Beskrivning av händelse

1.9 Budget

Typ av kostnad	Intern tid	Kostnad
Systemförvaltning		
Systemadministration		
Driftkostnad		
Årlig underhållskostnad (t ex Serviceavtal)		
Utvecklingskostnader (ska beskrivas i avsnitt 5.1)		
Planerade förvaltningsaktiviteter (ska beskrivas i avsnitt 5.2)		
Kostnader för utbildning (ska beskrivas i avsnitt 3.2)		
Övrigt		
SUMMA:		

Kommentarer kring budget

2 Systemförvaltningens organisation

2.1 Roller

Roll	Namn	Titel	Beräknad tidsåtgång (timmar per år)
Systemägare			
Systemförvaltare			
Systemadministratör			
Personuppgiftsansvarig			
Dataskyddsombud			
Dataskyddsamordnare			
Personuppgiftsbiträde			

2.2 Samverkan

Samverkan med	Orsak till samverkan	Form för samverkan

2.3 Integrationer

System	Beskrivning av och syfte med integration

3 Användarstöd

3.1 Support

Support kring IT-stödet ges av följande funktioner/personer:

Kontaktperson/Funktion	Tfn/e-post	Kommentar

3.2 Utbildning

4 Dokumentation

Dokumentation	Beskrivning	Sökväg

5 Utvecklings- och förvaltningsaktiviteter

5.1 Planerad utveckling av IT-stöd

Beskrivning av utveckling	Total kostnad	Varav resurser Servicecenter IT	Varav resurser systemleverantör, extern driftleverantör

5.2 Planerade förvaltningsaktiviteter

Tidpunkt	Aktivitet	Resurser systemförvaltning intern tid	Resurser Servicecenter IT	Resurser systemleverantör, extern drift-leverantör