# VÄGLEDANDE RÅD OCH BESTÄMMELSER – FÖRVALTNING & DRIFT AV IT INOM TIMRÅ KOMMUN

Fastställd av kommunstyrelsen 2016-12-06, § 292

## *Organisation och ansvar*

Förvaltningschef 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 informationssäkerhetspolicyns 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.

## *Definition av system*

Vad är ett system? För att klargöra för vilka system som gäller vad så har vi försökt att dela 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

## *IT-Forum*

IT-forum består av förvaltningschefer, systemförvaltare och centrala IT. Uppgifter är:

- 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 för konsulter och serviceföretag efter underlag från centrala IT och IT-säkerhetssamordnaren

## *Systemägare*

Systemägare måste finnas för alla slags 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 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 GAP-analys fastställa eventuella krav utöver basnivån. 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 Centrala IT 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 CIT
- 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 DISA 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 säkerhetsanalyser som respektive systemägare upprättat. Kraven i dessa planer ska vara koordinerade i systemsäkerhetsanalyser 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 (GAP-analys).

## 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 GAP-analys.

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 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 GAP-analys genomförs och följs upp årligen samt uppdateras 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:

- 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 skall hanteras ska finnas i GAP-analyserna. 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 beaktas både hur lösenorden skall vara beskaffade i form av längd och komplexitet men även hur byte av lösenord får ske
Konton bör använda sig av grupprättigheter i största möjliga utsträckning för att förenkla administrationen. Externa konsulter, vikarier och projektanställda skall ha tidsbegränsning på sina konton.
Användarna ska endast ges behörighet till det som är relevant för deras arbetsuppgifter. Avvikelse från detta skall loggas.

## 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 (GAP). 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 Centrala IT:

- 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 GAP-analysen 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 Centrala IT och systemägaren för beslut om vidare åtgärd.

### *Kommunikation*

Centrala IT 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 Centrala IT. 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
Namnstandarden bör bestå av komponenter som anger vad för typ av utrustning det är, verksamhetsområde och ett löpnummer.

### *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.