

# IT-strategi

för

## Hällefors kommun

---



---

Antagen av kommunfullmäktige 2005-06-07  
Reviderad 2010-02

# Innehåll

<b>1</b>	<b>BAKGRUND</b> .....	<b>3</b>
<b>2</b>	<b>SYFTE</b> .....	<b>3</b>
<b>3</b>	<b>INRIKTNINGSMÅL FÖR IT-VERKSAMHETEN</b> .....	<b>3</b>
<b>4</b>	<b>KRAV</b> .....	<b>4</b>
<b>5</b>	<b>ANSVARSFÖRDELNING</b> .....	<b>5</b>
	VERKSTÄLLIGHETSORGANISATION .....	6
	CENTRALA FUNKTIONER .....	6
	FÖRVALTNINGSFUNKTIONER .....	6
	EKONOMI, INKÖP, PLANERING.....	7
	FÖRVALTNINGARNA SVARAR FÖR KOSTNADER VAD GÄLLER: .....	7
	<i>Rutin för framtagande av anslagsäskande för datorutrustning</i> .....	7
<b>6</b>	<b>IT-SÄKERHET</b> .....	<b>7</b>
	BAKGRUND .....	7
	SYFTE.....	8
	MÅL .....	8
	KRAV .....	8
	GENOMFÖRANDE.....	9
	<b>SÄKERHETSPOLICY</b> .....	<b>9</b>
	<i>Datainformationssäkerhet</i> .....	9
	<i>Fysisk säkerhet</i> .....	9
	<i>Funktionssäkerhet</i> .....	9
	<b>DATASKYDD/BEHÖRIGHETS KONTROLL</b> .....	<b>10</b>



## 1 Bakgrund

Denna IT-strategi är övergripande för Hällefors kommun. Den ska vara vägledande för alla nämnder vid hantering av IT och IT-säkerhet inom kommunen.

Den mera ingående detaljstyrningen återfinns i dokumenten IT-säkerhetsinstruktioner: Förvaltning, Användare och Drift.

Med IT menar vi informationsteknik, vilket i ett ord sammanfattar alla informationshanterande processer inom en organisation så som datorer och moderna telefonsystem. Med IT-säkerhet menar vi de metoder och funktioner vi implementerar i organisationen och organisationens system som lösningar på de problem som hackerattacker, virus, stölder och andra hotbilder utgör.

## 2 Syfte

IT ska ses ur ett helhetsperspektiv för kommunen med en gemensam inriktning på IT-användandet för att uppnå bästa möjliga verksamhet åt kommuninnevånarna. IT-strategin skall ligga till grund för framtagande av IT-säkerhetsinstruktioner: Förvaltning, Användare och Drift. Som ligger till grund för systemsäkerhetsplanerna i de olika verksamhetssystemen

### IT-strategins syfte är att:

- Att uppnå BITS (Basnivå IT Säkerhet, Myndigheten för samhällsskydd och beredskaps rekommendationer för IT-säkerhet)
- Beskriva de regler som gäller för införande och hantering av IT i Hällefors kommun
- Ange riktlinjer och vägledning vid IT-anskaffning
- Följa den tekniska utvecklingen
- Skapa förutsättningar för kostnadseffektiv IT-verksamhet
- Skapa förståelse för IT-säkerhet i kommunen
- Skapa en gemensam skalbar teknisk plattform för IT

## 3 Inriktningsmål för IT-verksamheten

- Användandet av IT skall medverka till att ge medborgarna en god och effektiv samhällsservice.
- Användandet av IT skall ge beslutsfattare på alla nivåer ett bra beslutsunderlag med data av god kvalitet.



- Användandet av IT skall tillgodose de anställdas behov av en god arbetsmiljö samt främja personalutvecklingen och ge motivation och effektivitet i arbetet.
- Användandet av IT skall vara ett hjälpmedel för en bra verksamhetsstyrning och bidra till effektivt resursutnyttjande och kostnadseffektivitet samt ge enklare och effektivare rutiner.
- Lagstadgade krav för offentlighet och sekretess samt för behandling av personuppgifter skall uppfyllas.
- IT-strategin skall vara förankrad både politiskt och hos de anställda.
- IT-strategin skall medverka till att kommunen uppnår målet med 24-timmars myndigheten.
- Användandet av IT skall vara demokratifrämjande.

## 4 Krav

Strategin skall utvärderas varje år och vid behov revideras.

IT-planen skall revideras vid behov.

Varje nämnd skall ha en IT-säkerhetsplan som knyts till IT-strategin och som mer i detalj beskriver hur IT-strategin skall förverkligas.

Konsekvenserna ska analyseras och värderas före beslut om införande av IT-system, samt följas upp och utvärderas enligt fastställd tidplan

Systeminförande, gemensamma eller förvaltningsspecifika, ska analyseras och bedömas tillsammans med kommunens IT-enhet och i möjligaste mån samordnas

### **IT-planen ska behandla:**

- Systemutbyggnad d.v.s. större systemförändringar eller planerade upphandlingar av nya system, ej årliga uppdateringar
- Systemansvar
- Utrustningsbehov
- Budgetfrågor
- Tidplaner
- Arbetsmiljö
- Utbildningsbehov

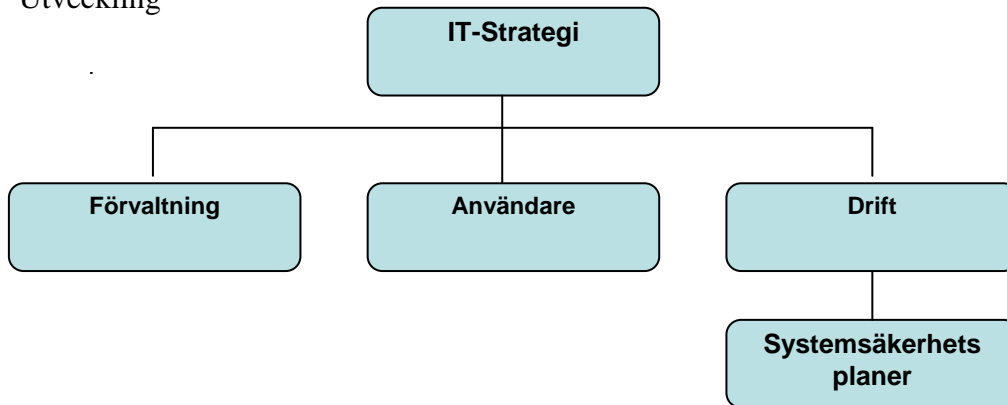
### **IT-planen skall vidare beskriva:**

- Uppsatta mål och färdriktning
- Praktisk och teknisk realisering



**Krav som skall beaktas:**

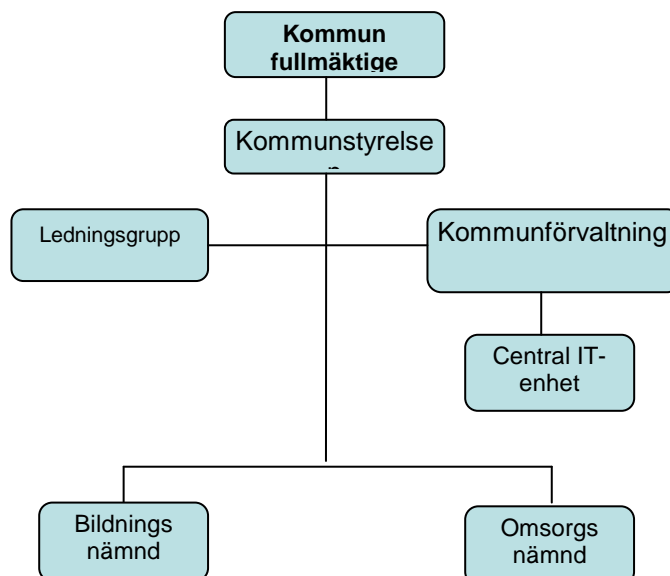
- Samverkan inom kommunen och i KNÖL
- Säkerhet inom kommunen och i KNÖL
- Funktionalitet inom kommunen och i KNÖL
- Arbetsmiljö
- Utveckling



## 5 Ansvarsfördelning

Kommunstyrelsen har det politiska, övergripande ansvaret för IT-strategin. Till sin hjälp har den en tjänstemannagrupp, IT-gruppen, vars uppgift är att informera, vara rådgivande, samordna, engagera och stötta förvaltningarna i deras arbete.

Varje nämnd har huvudansvaret i IT-frågor rörande sin egen verksamhet. Delegering till förvaltningar och/eller verksamhetsansvariga för genomförande av beslut frångår inte nämndens ansvar.





## Verkställighetsorganisation

Nedan anges de funktioner som ska finnas inom IT-området i kommunen. För detaljerade funktions- och ansvarsbeskrivningar beslutar respektive nämnd. Samma person kan inneha flera av angivna funktioner och roller. Kommunstyrelsen fastställer riktlinjer för vilka krav som ska gälla för olika funktioner.

## IT-grupp

IT-gruppens funktion är att vara informationskontakt och rådgivande organ, samt diskussionsforum i IT-frågor.

## Samarbets-/projektgrupper

IT-gruppen inrättar samarbetsgrupper eller projektgrupper efter behov och ska också ange ändamålet för gruppernas verksamhet.

## Systemansvar

För system som övergriper flera förvaltningar ska det utses en systemförvaltare per system. Vid eventuella oklarheter beträffande ansvaret fattas beslutet av kommunstyrelsen.

## Varje system skall ha en systemförvaltare

Systemförvaltare skall utses av systemägaren med skriftlig delegation. Systemförvaltaren kan i sin tur ha flera systemadministratörer.

## Centrala Funktioner

Under kommunförvaltningen ska finnas en central IT-enhet med övergripande ansvar för planering, utveckling, drift och säkerhet för IT-verksamheten inklusive gemensam utbildning.

## Förvaltningsfunktioner

Under nämnd/förvaltning ansvarar systemansvarig för den operativa IT-verksamheten inom förvaltningen, innefattande planering, utveckling, drift, säkerhet och utbildning.

## Följande funktioner ska finnas:

- Systemägare
- Kontaktpersoner mot central IT-enhet och IT-ansvarig
- Säkerhetsansvariga
- IT-utbildningsansvariga



### **Ekonomi, inköp, planering**

Upphandling av system skall göras i samråd med kommunens IT-enhet och IT-gruppen.

IT-investeringar skall därför ske genom en samordnad planering med IT-enheten.

Inköp av datorutrustning såsom datorer, skrivare, skanners, digitalkameror, licenser etc. ska ske via IT-enheten. Gäller alla produkter som ska kopplas till datanätet.

Kostnaderna för kommunens gemensamma resurser inom IT-området skall bäras av de verksamheter som nyttjar dessa.

### **Förvaltningarna svarar för kostnader vad gäller:**

- Arbetsplatsutrustning
- Standardsystem
- Förvaltningsspecifika system
- Utbildning
- Datorutrustning
- Teknisksupport och mjukvarusupport

### **Rutin för framtagande av anslagsäskande för datorutrustning**

- Behov av inköp av dataprodukt initieras av respektive förvaltning som också upprättar kravspecifikation.
- Samråd sker med IT-enheten om
  - teknisk lösning (datorer, skrivare, kommunikation, etc.)
  - mjukvara, integrationsmöjligheter, kompatibilitet etc.
  - driftkostnader
- Respektive facknämnd begär anslag i sitt budgetförslag eller i samråd med IT-enheten
- IT-enheten gör en bedömning av samtliga anslagsäskanden och behandling sker i IT-gruppen

## **6 IT-säkerhet**

### **Bakgrund**

Kommunen använder IT för att stödja och utveckla verksamheten. Den tekniska utvecklingen innebär allt mer integrerade och avancerade IT-system. Kraven på snabb och relevant information ökar. Informationen ska dessutom i mycket stor utsträckning vara tillgänglig för allmänheten (offentlighetsprincipen).

IT-säkerheten rör all hantering av information i datamiljö.



## Syfte

För att tillgodose de krav som ställs på den information vilken behandlas i kommunens IT-system är det nödvändigt att informationshanteringen sker på ett så tillförlitligt sätt som möjligt.

IT-säkerheten syftar till att förebygga och minimera oönskade konsekvenser av skiftande art inom kommunens IT-verksamhet, t ex otillåten åtkomst av information, virusattacker, eller hackerattacker.

## Mål

### Målet för IT-säkerhetsarbetet i Hällefors kommun är att

- kontinuerligt göra riskanalyser med hjälp av dokumentet "IT-säkerhetsinstruktioner: Förvaltning, Drift, Användare" och därigenom få underlag för bedömning av säkerhetsåtgärder enligt IT-strategin (enl.BITS).
- tillsammans med IT-enheten hitta lösningar för att minska eller åtgärda ev. risker
- säkerheten ska ha sådan nivå att all information som behandlas ska skyddas på bästa sätt
- ge IT-användare i Hällefors kommun förståelse för vikten av säkerhetstänkande vid all hantering av information
- alla anställda i Hällefors kommun ska känna till de lagar och bestämmelser samt förstå innebörden av dessa.
- Följa uppställda mål och krav i dokumentet "IT-säkerhetsinstruktioner: Förvaltning"
- Följa uppställda mål och krav i dokumentet "IT-säkerhetsinstruktioner: Drift"
- Följa uppställda mål och krav i dokumentet "IT-säkerhetsinstruktioner: Användare"

## Krav

### Alla IT-användare inom Hällefors kommuns förvaltningar ska:

- följa säkerhetsreglerna
- ha kunskaper om de lagar och bestämmelser som gäller för området som t ex tystnadsplikten, Pul (personuppgiftslagen)

Till grund för IT-säkerhetsåtgärder ska föreligga dokumenterade riskanalyser.

IT-säkerheten ska innefatta såväl täcka obehörig läsning och förändring av, samt förlust av information

Uppföljning av riskanalyser och skyddsåtgärder och utbildningsinsatser ska ske kontinuerligt



## Genomförande

### För att uppnå uppsatta säkerhets mål ska följande utföras:

- Riskbedömningar inklusive konsekvensanalyser
- Riskanalys ska utföras som en del i risk och sårbarhets arbetet i Hällefors kommun
- IT-säkerhetshöjande åtgärder
- Utbildning och information
- Incidenter som innebär hot mot datasäkerhet ska anmälas till IT-ansvarig.

## Säkerhetsstrategi

Följande säkerhetsområden ska beaktas:

### Datainformationssäkerhet

För att undvika dataintrång, förlust av data, obehörig förändring av data, avslöjande av information och dylikt ska åtgärder av mer administrativ karaktär utföras såsom :

- Lösenordsskydd
- Virusprogram
- Rättigheter
- Ansvarsfördelning
- Kryptering
- Backup-programvara
- Katastrofplan
- Information om tystnadsplikt /PUL (Personuppgiftslagen)
- Vid konsultation av extern personal ska avtal skrivas om tystnadsplikt

### Fysisk säkerhet

Åtgärder för fysisk säkerhet för att undvika obehörigt tillträde, brand, översvämningar/vattenläckage, sabotage, stöld m.m. utgörs av mer teknisk karaktär:

- Inpasseringskontroll
- Brandskydd / brandlarm
- Översvämningsskydd
- Stöldskydd

### Funktionssäkerhet

Funktionssäkerhet menas skydd mot olika typer av driftsstörningar i datanätet och system. Åtgärderna är delvis av teknisk karaktär och innebär:

- Dubblerade utrustningar (s.k. kluster)



- Kylanläggning
- Reservkraft
- UPS (avbrottsfri kraft)
- Åskskydd
- Brandvägg
- Backuprobot
- Skydd kan ordnas också genom serviceavtal
- Övervakningssystem

## Dataskydd/behörighets kontroll

Åtgärder för att förhindra åtkomst, otillåten förändring eller sabotage av data utförs enligt följande:

- Alla användare ska ha en unik användaridentitet.
- Alla användare ska ha ett lösenord som **endast** är känt för användaren själv.
- Lösenordet ska bestå av minst 6 tecken (bokstäver, siffror \*, \_ / & ! ? > < får användas). Lösenordet ska inte kunna knytas till användaren på något sätt d.v.s. lösenordet ska inte vara namn på ex anhöriga, husdjur eller personnummer.
- **Lösenordet får inte "lånas ut" till någon annan anställd eller utomstående.**
- Lösenordet ska ej skrivas ned.
- Tillgång till systemet ska spärras efter maximalt 5 försök med felaktiga lösenord. Denna spärr ska endast kunna hävas av behörighetsansvarig.
- Användarna ska själva byta lösenord med vissa intervall anpassat efter verksamhetens krav.
- Det nya lösenordet får inte vara samma som det föregående.
- Behörighet ska tidspreciseras för vikarie och visstidsanställda.
- Vid avslutad tjänst låses kontot och efter en månad tas e-post kontot bort. Under den månaden ska e-posten vidarebefordras till annan anställd inom förvaltningen.
- För att undvika intrång ska datorn "låsas"<sup>1</sup> när arbetsplatsen lämnas. (Gäller från Windows 2000). På äldre system gäller att man loggar ut ur nätet.
- Det är inte tillåtet att ansluta utrustning i nätverket utan skriftligt tillstånd från IT-enheten.

---

<sup>1</sup> Genom att trycka ned tangenterna ctrl+alt+del och trycka enter låser man datorn.