

2008-09-15

Kst 2008/351.01



# Informationssäkerhet i Torsby kommun

Säkerhetsplan

Ver 2

20080915

## Allmänt om informationssäkerhet

Information är en av våra viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med Torsby kommuns risk- och sårbarhetsanalys.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar, förordningar och föreskrifter
- Våra egna krav
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar Torsby kommuns informationstillgångar utan undantag.

Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- att informationen är och förblir riktig

Informationssäkerheten är en integrerad del av vår verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar.

Alla delar inom Torsby kommun är bundna av denna informationssäkerhetsplan vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Den som använder våra informationstillgångar på ett sätt som strider mot denna plan kan bli föremål för disciplinära åtgärder

### Mål för informationssäkerheten

Torsby kommun skall bedriva ett **aktivt** informationssäkerhetsarbete i syfte att säkerställa kommunens information. Verksamhetens krav på information och informationssystemens tillgänglighet skall tillgodoses.

Målsättningen med **informationssäkerheten** är att säkerställa Torsby kommuns verksamhet mot avbrott och minska skadorna på verksamheten genom att **förebygga** och **minimera** verkan av oönskade händelser.

Nedanstående åtgärder skall utföras för att nå målet:

- Informationens **riktighet** skall säkerställas. (Regleras genom respektive systemsäkerhetsplan.)

- Informationens **tillgänglighet** skall säkerställas. (Regleras genom respektive systemsäkerhetsplan.)
- Informationens **sekretess** skall säkerställas. (Regleras genom respektive systemsäkerhetsplan.)
- Informationens **spårbarhet** skall säkerställas. (Regleras genom respektive systemsäkerhetsplan.)
- Krav i **lagar och avtal** skall uppfyllas. (bl.a. PuL, Offentlighetslagen, Upphovsrättslagen, Sekretesslagen)
- Rekommendationer från Krisberedskapsmyndigheten enligt **Basnivå för IT-säkerhet (BITS) utgåva 3** skall följas i största möjliga utsträckning..
- Utbildning i informationssäkerhet skall ges alla anställda.
- Alla **säkerhetsincidenter**, konstaterade eller misstänkta, skall rapporteras till och undersökas av **informationssäkerhetsansvarige**.
- Samtliga anställda skall ha tagit del av denna plan samt skriften "IT-regler för Torsby kommun".

Som ett led i måluppfyllelsen skall följande dokument upprättas:

- **Övergripande systemsäkerhetsplan** ansvarig IT-avdelningen.
- **Systemsäkerhetsplan**, ansvarig är respektive nämnd/systemägare.
- **Avbrottsplan**, ansvarig är respektive nämnd/systemägare.
- **Säkerhetsinstruktioner och Kontinuitetsplan**, ansvarig för upprättande är IT-avdelningen
- **Användarpolicy** ("IT-regler för Torsby kommun") till stöd för denna policy. Dessa dokument omfattar administrativa rutiner, hantering av tekniska hjälpmedel (ex. e-post, antiviruslösningar) och säkerställande av fysiskt skydd (ex. lås och larm). Ansvarig för upprättande är IT-avdelningen. Skall fastställas av Kommunstyrelsen.

## Motiv

Informationssäkerhet syftar till att **skydda kommunens informationstillgångar** som omfattar datorer, system, kommunikation, material, kapital, personal, lokaler, goodwill och **informationsbehandlingsresurser** mot **alla hot**.

Informationssäkerhetsarbetet görs för att säkerställa verksamhetens kontinuitet, minska skador på verksamheten och maximera avkastningen på investerat kapital.

## Ansvar

- Kommunstyrelsen fastställer informationssäkerhetsplanen och är ytterst ansvarig för dess efterlevnad.
- Kommunchefen har centralt informationssäkerhetsansvar och biträds av utsedd informationssäkerhetssamordnare.
- Funktionen och ansvaret för att leda informationssäkerhetsarbetet tilldelas informationssäkerhetssamordnaren.
- Informationssäkerhetssamordnaren har det direkta ansvaret för att vidmakthålla denna plan och att ge råd och vägledning för dess införande.
- Nämndeordföranden tillika systemägaren är direkt ansvariga för att denna plan följs inom sina respektive system och för sin personals efterlevnad av den.
- IT-avdelningen ansvarar för Säkerhetsinstruktionen och Kontinuitetsplanen.
- Det är varje anställds ansvar att efterleva kommunens informationssäkerhetsplan.

## Generella krav

Torsby kommuns informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Alla informationssystem ska minst klara den basnivå för informationssäkerhet som Krisberedskapsmyndigheten rekommenderar (BITS).

Vissa informationssystem är en *förutsättning* för att kunna bedriva vår verksamhet. För dessa ska en riskanalys upprättas med stöd av Krisberedskapsmyndighetens verktyg för analys av informationssäkerhet (BITS Plus). Analysen ska utgöra underlag för driftgodkännande och fastställas av Kommunstyrelsen. Information i dessa system skall klassificeras med avseende på sekretess, riktighet, tillgänglighet och spårbarhet enligt kommunens klassningsmodell.

## Distansarbete

För att personalen ska kunna arbeta effektivt ska möjlighet finnas att arbeta mobilt eller stationärt på distans. Förutsättningar och restriktioner för detta ska dokumenteras.

## Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- regler följs
- att planer, säkerhetsinstruktioner och riskanalyser vid behov revideras.

## **Definitioner**

Information förekommer i många former – tryckt, skriven, elektroniskt lagrad, skickad med post eller e-post, visad på film eller talad.

*Riktighet* – skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga.

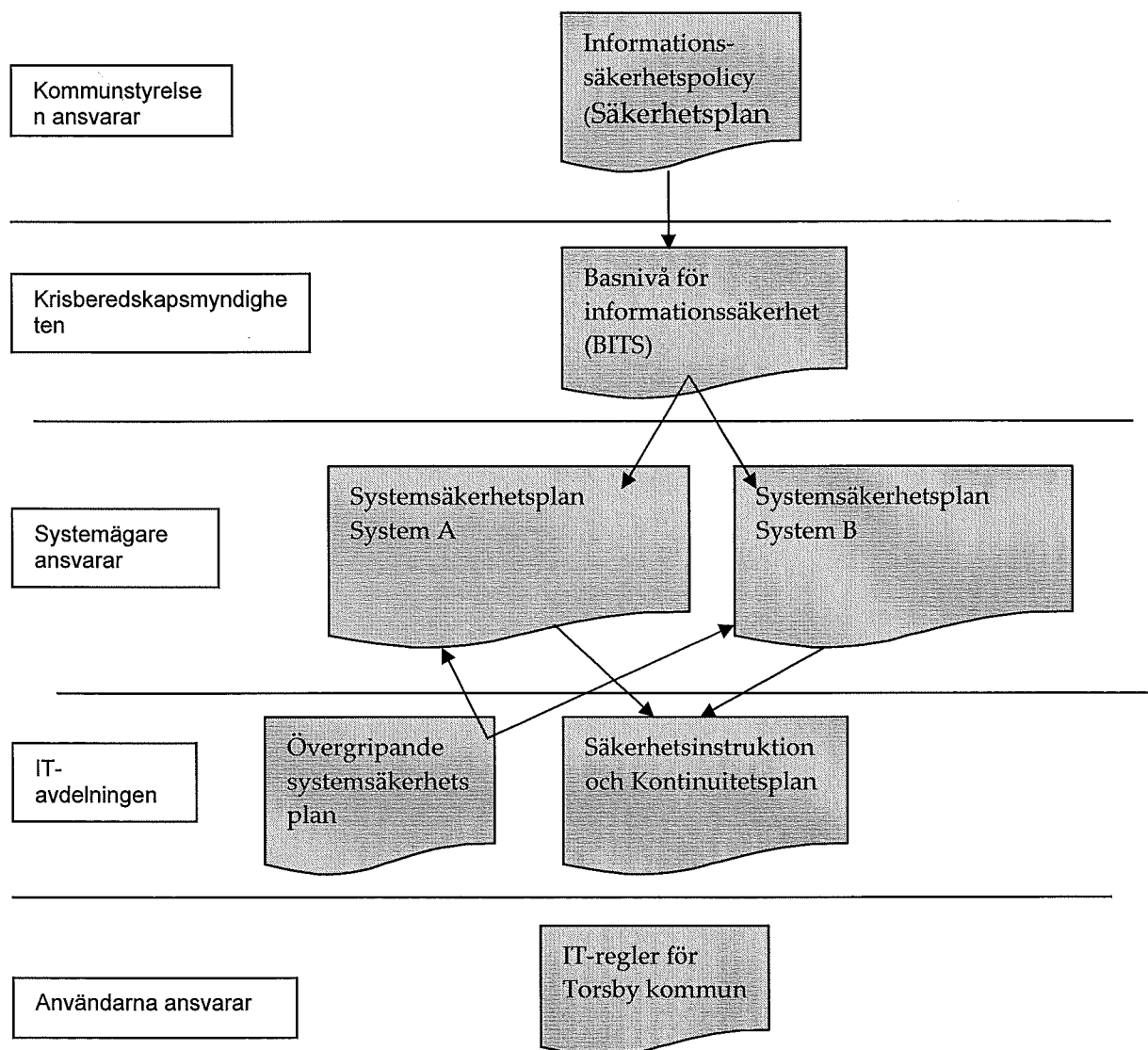
*Tillgänglighet* – säkerställande av att behöriga användare vid behov har tillgång till information och tillhörande tillgångar.

*Sekretess* – säkerställande av att information är tillgänglig endast för dem som har behörighet för åtkomst.

*Spårbarhet* – Att med hjälp av loggning kunna se vilka förändringar som har gjorts i systemen och vem som har utfört dessa.

**Bil. 1**

Nedanstående skiss visar samtliga dokument som ingår i kommunens informationssäkerhetsarbete.



**Informationssäkerhetsplanen** visar inriktning på ett övergripande plan. Dokumentet syftar till att visa att kommunen skall bedriva ett informationssäkerhetsarbete och vilka huvudmål man vill uppnå.

**Basnivå för informationssäkerhet (BITS)** framställs och underhålls av Krisberedskapsmyndigheten.

**Övergripande systemsäkerhetsplanen** förtecknar alla i kommunen förekommande system samt prioriterar och klassificerar dem enligt klassningsmodellen.

**Systemsäkerhetsplanerna** är individuella planer för varje enskilt system där ägarna av systemen (nämnderna) i icke tekniska termer beskriver systemen och vilka säkerhetsmässiga krav som ställs på systemen utifrån ett helhets perspektiv. Det kan vara krav på när systemen skall vara tillgängliga, sekretessnivå och nivå på riktighet. Skall innehålla en avbrottsplan för alternativ drift. Här beskrivs även vilka som har rätt att dela ut behörigheter till systemen.

**Säkerhetsinstruktionerna** är konkreta regler och rutiner avseende IT-säkerhet som förvaltaren av systemen (IT-avdelningen) sätter samman utifrån de krav som systemägare specificerat i sina systemsäkerhetsplaner och riktar sig till användare och driftpersonal eller personal för administration och förvaltning.

**Kontinuitetsplanen** kan i dokumenterad form t.ex. innehålla:  
Villkor för aktivering av planen, larm, åtgärder/avbrottsplan, aktivering av reservrutiner, återgång till normal drift, informationsspridning etc.

**IT-regler för Torsby kommun** är en instruktion till alla användare av kommunens system och är ett regelverk för hur kommunens information och informationsresurser får användas. Det ligger på varje förvaltnings ansvar att tillse att alla anställda tar del av dessa regler samt efterlever dem. För att få behörighet till kommunens nätverk skall en bilaga till IT-reglerna undertecknas och insändas till IT-avdelningen.