TANUMS
KOMMUN

Riktlinjer för informationssäkerhet

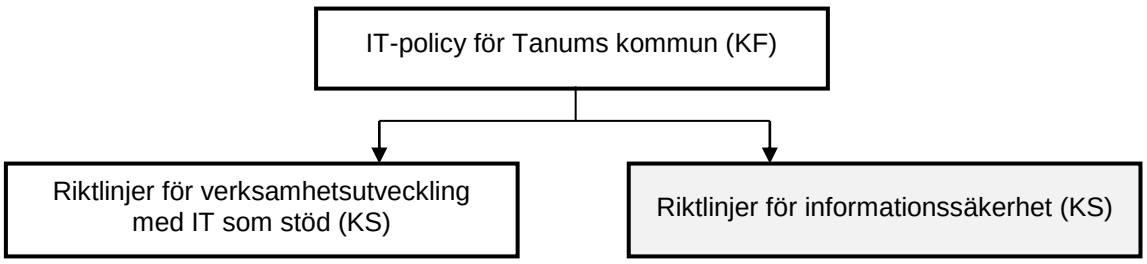
ver 1.0

Antagen av Kommunstyrelsen 2013-05-29

1. Inledning

Tanums kommuns övergripande styrdokument inom IT-området är ***IT-policy för Tanums kommun.*** Policyn är antagen av Tanums kommunfullmäktigen den 18 mars 2013. Policyn anger kommunens förhållningssätt till och inriktningen för användning och utveckling av informations- och kommunikationsteknik för att utveckla kommunens verksamheter och för att bidra till att nå kommunens mål och göra det på ett informationssäkert sätt. IT-policyn förvaltas av Kommunstyrelsen.

Föreliggande dokument behandlar informationssäkerheten inom IT-verksamheten.



IT-policyn och kommunstyrelsens bägge dokument för riktlinjer för IT gäller för hela Tanums kommun med dess bolag. Med begreppet Tanums kommun avses i fortsättningen både kommunen och bolagen.

2. Kommunfullmäktiges antagna mål och roller

2.1 Mål för IT-verksamheten

Kommunfullmäktige har beslutat att de övergripande målen för verksamhetsutveckling med IT som stöd är att:

- kommunen skall erbjuda e-tjänster till nytta för invånare, näringsliv och organisationer för att ge kvalitativ och effektiv service
- anställda och politiker inom kommunen skall ges de kunskaper och de verktyg som krävs för att kostadseffektivt utnyttja modern informationsteknologi
- användningen av IT skall vara ett redskap i verksamhetsutveckling samt ge möjlighet till effektiv samverkan inom kommunen och med andra kommuner, Region, statliga förvaltningar och andra organisationer där relationen påverkar medborgarnas nytta
- kommunen skall i samverkan med övriga kommuner i regionen, Region och leverantörer samt utförare erbjuda service som utgår från invånarens livssituation
- kommunens IT-verksamhet skall präglas av höga ambitioner vad avser informationssäkerhet och tillgänglighet
- Tanums kommun skall ha en sammanhållen och därmed kostadseffektiv IT-verksamhet

2.2 Roller och ansvarsområden för IT-verksamheten

Kommunfullmäktige har i sin IT-policy beslutat om följande ansvarsfördelning:

Kommunfullmäktige

- beslutar om för kommunen gemensam IT-policy

. Kommunstyrelsen ansvarar för att:

- IT-verksamheten bedrivs så att kommunfullmäktiges mål för IT-verksamheten uppnås
- IT-verksamheten effektivt tillgodoser kommunens gemensamma behov och att den bedrivs med rätt krav på säkerhet och skydd av personlig integritet

- besluta om vilken information och vilka IT-system som skall vara gemensamma för kommunen
- genom kommunstyrelsens stab styra, samordna och vidareutveckla kommunens IT-verksamhet

Kommunstyrelsen är ägare av de kommungemensamma IT-systemen, såväl hårdvara som mjukvara.

3. Kommunstyrelsens syfte med Riktlinjer för informationssäkerhet

Riktlinjen redovisar ledningens viljeyttring och engagemang gällande informationssäkerhetsarbetet och syftar till att sammanfatta och tydliggöra den säkerhetsnivå som Tanums kommuns IT-verksamhet skall ha och vad som skall gälla för roller och ansvarsfördelning samt revision.

Inom Tanums kommun skall informationssäkerhetsarbetet utifrån MSB:s[i] kvalitetssäkringsmodell, BITS[ii] basnivå.

3.1 Om information och informationssäkerhet

Information är en av Tanums kommuns viktigaste tillgångar. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten är en integrerad del av vår verksamhet. Med informationssäkerhet menas den samlade effekten av de skyddsåtgärder, som tillsammans minskar eller eliminerar de hot och risker, som riktar sig mot IT-stödet och informationsresurserna.

Informationssäkerhet handlar om:

- *Sekretess*, skydd mot obehörig åtkomst av information
- *Riktighet*, åtgärder för att åstadkomma rätt kvalitet på information
- *Tillgänglighe*t, åtgärder för att säkra drift och funktionalitet
- *Spårbarhet*, möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse

Utgångspunkten för arbete med informationssäkerhet är lagar, avtal, förordningar och föreskrifter samt kommunens egna krav. De reglerar hur kommunen, och andra nyttjare av kommunens informationstillgångar och IT-infrastruktur skall arbeta med informationssäkerhet. Personer som omfattas är förtroendevalda, anställda och i viss omfattning skolelever samt konsulter / entreprenörer om deras uppdrag är relevanta för kommunens informationssäkerhet. Regler och organisation kring IT-säkerhet skall vara känd för alla berörda och efterlevnaden skall följas upp kontinuerligt.

Förankringen och medvetandet hos medarbetarna utgör själva grunden för informationssäkerhetsarbetet.

Tanums kommun har valt att bygga upp strukturen för informationssäkerhet med stöd av nationella rekommendationer som finns publicerade.

Tillämpning av kommunens riktlinjer för informationssäkerhet gäller för alla system oavsett ägande verksamhet och innebär att:

- Grundnivån för säkerheten skall fastställas genom informationsklassificering

- Skydd skall anpassas efter genomförd riskanalys
- Åtkomst/behörighet skall tilldelas formellt och endast efter behov
- Beslut om åtkomst/behörighet skall dokumenteras
- Anställdas åtkomst/behörighet skall följas upp regelbundet
- Alla incidenter skall rapporteras och kontinuerlig uppföljning skall ske mot fastställda regler

4. Kommunstyrelsens mål för IT-verksamheten

4.1 Övergripande ansvar

De övergripande mål för verksamhetsutveckling med IT som stöd är:

- Tanums kommun skall erbjuda e-tjänster till nytta för invånare, näringsliv och organisationer för att ge kvalitativ och effektiv service
- anställda och politiker inom Tanums kommun skall ges de kunskaper och de verktyg som krävs för att kostadseffektivt utnyttja modern informationsteknologi
- användningen av IT skall effektivisera Tanums kommuns verksamheter och vara ett redskap i verksamhetsutveckling samt ge möjlighet till effektiv samverkan inom kommunen och med andra kommuner, Region, statliga förvaltningar och andra organisationer där relationen påverkar medborgarnas nytta
- Tanums kommun skall i samverkan med övriga kommuner i regionen, Region och leverantörer samt utförare erbjuda service som utgår från invånarens livssituation
- ***Tanums kommuns IT-verksamhet skall präglas av höga ambitioner vad avser informationssäkerhet***
- Tanums kommun skall ha en sammanhållen och därmed kostadseffektiv IT-verksamhet

Det övergripande målet för IT-säkerhetsarbetet är:

- att genom ett strukturerat och väl genomtänkt informationssäkerhetsarbete skydda kommunens information mot oönskade händelser som ger negativa konsekvenser för verksamhet, medborgare och samverkan.

4.1.1 Roller/ansvar för informationssäkerhet

- **Kommunstyrelsen** har det övergripande ansvaret
- **Kommunstyrelsens stab** har det övergripande operativa ansvaret
- **Nämnd och bolag** har ansvar inom respektive verksamhetsområde
- **Förvaltningschef/VD** organiserar informationssäkerhetsarbetet inom förvaltningen/bolaget samt ansvarar för ledning och kontroll. FC/VD är system-/ objektsägare och har det övergripande förvaltaransvaret för verksamhetssystem
- **Objektsägare,** normalt förvaltningschef eller VD, är ansvariga inom respektive område. För IT-infrastruktur är IT-chefen objektsägare Dessa skall själva planera så att resurser avsätts för att policy, riktlinjer och rutiner kan följas
- **Systemförvaltaren** har det dagliga ansvaret för systemanvändandet på verksamhetsnivå. För systemförvaltare skall finnas utpekad ersättare. Systemförvaltaren har en tilldelad IT-tekniker med ersättare som resurs för den tekniska systemdriften.
- **IT-chef** är övergripande ansvarig för att beslutade åtgärder gällande infrastruktur och skydd av gemensamma resurser genomförs. IT-chefen är objektsägare för IT-infrastrukturen och rapporterar till Kommunstyrelsens stab.

- **Informationssäkerhetssamordnare** är ansvarig för att samordna informationssäkerhetsarbetet inom kommunen. Inom Tanums kommun svarar kommunstyrelsens stab som informationssäkerhetssamordnare

- **Användare** ansvarar för att följa kommunens gällande riktlinjer och instruktioner

4.1.2 Uppdrag till verksamheten

- **Kommunens informationssystem**
  Samtliga informationssystem skall vara identifierade, förtecknade och bedömda efter vilka som är verksamhetskritiska. Av förteckningen skall en fullständig roll- och ansvarsbeskrivning framgå för identifierade system. Alla informationssystem skall minst klara den basnivå för informationssäkerhet som kommunen fattat beslut om.

- **Informationsklassificering av verksamhetssystem**
  För samtliga verksamhetssystem skall en informationsklassificering göras. Utifrån klassificeringen skall regler för säkerhet och tillgänglighet (t ex tillgänglighet via fjärkommunikation) fastställas.

- **Systemsäkerhetsanalyser**
  Systemsäkerhetsanalyser skall genomföras på identifierade verksamhetskritiska informationssystem.

- **Riskbedömningar**
  Hotbilden för varje enskilt informationssystem som är av vikt för verksamheten skall analyseras fortlöpande, och identifierade händelser som kan leda till negativa konsekvenser skall förebyggas.

- **Incidenthantering**
  Skade- och incidentrapporteringsrutin skall finnas inom Tanums kommun och följas av verksamheten.

- **Informationssäkerhetsutbildning - Introduktionsutbildning**
  All personal skall i samband med nyanställning, omplacering och när speciellt behov föreligger få den utbildning som behövs för att informationssäkerheten skall upprätthållas.

4.2 Kommunstyrelsens stabs ansvar

Kommunstyrelsens stab ansvarar för de strategiska frågorna kring IT-användning, IT-utveckling och IT-säkerhet. Kommunstyrelsens stab skall skapa förutsättningar för verksamhetsutveckling med stöd av IT i kommunen.

Kommunstyrelsen uppdrar åt Kommunstyrelsens stab att ansvara för att:

- på en övergripande nivå analysera utvecklingen inom IT-området
- upprätta en väl fungerande samverkan med förvaltningar och bolag inom IT-området så att insatser kan värderas, prioriteras och ges en nyttokalkyl i relation till mål från kommunfullmäktige
- stödja kommunstyrelsen i samordningen av strategiska projekt inom IT-området
- genomföra en ökad samordning inom IT-området med fokus på nytta för verksamheten
- samordna och förstärka utvecklingen av e-tjänster
- på en övergripande nivå analysera kommunens IT-verksamhet och föreslå åtgärder för ekonomisk effektivisering
- analysera nyttan med IT-stödet och utifrån nyttoanalysen ta fram förslag till förändring
- ta initiativ som leder till en ökad grad av konsolidering och standardisering

- långsiktigt planera och samordna interna och externa leveranser av IT-tjänster till kommunens verksamheter för en stabil och kostnadseffektiv IT-verksamhet
- medverka till att effektivisera kommunens administration och verksamhet med hjälp av IT
- fastställa kommungemensamma standarder för IT inom Tanums kommun
- ***fastställa föreskrifter och genomföra regelbundna revisioner av IT-säkerhetspolicyn***
- ***tillse att de av kommunstyrelsen ägda systemen hanteras enligt gällande riktlinjer***
- organisera Styrgrupp IT:s verksamhet
- använda Styrgrupp IT för att inhämta IT-relaterad information inför beslut samt att sprida sådan information i organisationen
- organisera IT-enhetens verksamhet. IT-enheten är underställd ekonomikontoret.

4.3 Nämnders, styrelsers och bolags ansvar

Nämnder, styrelser och bolag ansvarar för att IT-policyn samt av Kommunstyrelsens och Kommunstyrelsens stabs anvisningar för verksamhetsutveckling med IT och riktlinjer vad gäller IT-säkerhet som stöd efterföljs. Den egna verksamhetens lokala riktlinjer och handlingsplaner skall anpassas till den övergripande policyn. Detta skall vara en del i verksamhetsplanering och uppföljning inom kommunens integrerade ledningssystem.

Nämnder, styrelser och bolag ansvarar vidare för att:

- IT-verksamheten inom nämnden bedrivs med rätt krav på säkerhet, skydd av personlig integritet och förtroende hos allmänheten
- ***hantering av personuppgifter sker i enlighet med sekretesslagen samt personuppgiftslagen***
- ***nämnden utser en för varje ägt verksamhetssystem en systemförvaltare med ersättare***
- organisationen genom systemförvaltaren och dennes ersättare har kunskap om ägda system
- ***information som rör egen verksamhet i gemensamma system är korrekt***
- IT-verksamheten inom nämndens verksamhetsområde effektivt tillgodoser såväl kommunens gemensamma som de enskilda verksamheternas behov
- ***de regler och riktlinjer som utfärdas skall spridas och implementeras inom förvaltningar och bolag***
- förvaltningar och bolag deltar i det samarbete som bedrivs i gemensamma IT-frågor
- ***all berörd personal har tillräcklig utbildning och tydliga instruktioner för att genomföra sina arbetsuppgifter i samband med användning av IT på ett effektivt och säkert sätt***
- Ta hänsyn till den psykosociala arbetsmiljön när verksamheterna förändras med IT-stöd och att den ergonomiska arbetsmiljön är lämpligt utformad
- det sker en kontinuerlig uppföljning av att föreskrivna regler tillämpas av alla anställda inom verksamheten
- ***det sker en kontinuerlig uppföljning av att föreskrivna regler tillämpas för de av förvaltningen ägda verksamhetsystemen***

5. Uppföljning och översyn

Förvaltningschefer och VD:ar för de kommunala bolagen är ansvariga för att denna policy efterföljs och kontinuerligt följs upp. Kommunstyrelsens stab ansvarar för att det finns direktiv och regelverk för hur uppföljning och översyn skall genomföras.

Kommunens/och bolagens revisorer beslutar om åtgärder för att granska informationssäkerhetsarbetet och i samband med revision följa huruvida

- beslutade åtgärder är genomförda
- granskning av kommunikationsresurser, IT-system och datorer utförs
- säkerhetsfrågor beaktas vid upprättande av kravspecifikationer och servicenivåavtal
- riktlinje och säkerhetsinstruktioner följs

- riktlinje, säkerhetsinstruktioner och riskanalyser vid behov revideras.

[i] MSB= Myndigheten för samhällsskydd och beredskap

[ii] BITS= Basnivå för informationssäkerhet. BITS är samlingsnamnet på MSB:s rekommendationer för hur en organisation kan ta ett helhetsgrepp på informationssäkerhet.
[https://www.msb.se/sv/produkter--tjanster/informationssakerhet---stod--verktyg/bits-konceptet/]