



ÖVERKALIX  
KOMMUN

# Policy för Informationssäkerhet i Överkalix kommun

---

**Postadress**

956 81 ÖVERKALIX

**Internet:** [www.overkalix.se](http://www.overkalix.se)

**Besöksadress**

Storgatan 17

**Telefon**

0926-740 00

**E-post:** [kommun@overkalix.se](mailto:kommun@overkalix.se)

**Telefax**

0926-77920

**Bankgiro**

757-9311



## Bakgrund

### Policy för informationssäkerhet i Överkalix kommun

Denna policy ska redovisa viljeinriktning från den kommunala politiska ledningen i Överkalix kommun. Med policyn beskrivs även ansvar, roller, metoder och mål för informationssäkerhetsarbetet i kommunen. Policy för informationssäkerhet i Överkalix kommun fastställs av kommunfullmäktige och kommuniceras till samtliga anställda vid kommunen och relevanta externa parter. Policyn ska vara känd och tillgänglig i aktuell version på kommunens intranät och på kommunens hemsida. Avtal och överenskommelser får inte skrivas för eller av Överkalix kommunen som åsidosätter kraven i denna policy.

### Vad är informationssäkerhet, och varför är det viktigt för oss att arbeta med?

Information är en av kommunens viktigaste resurser och behöver därför skyddas. Alla kommunens verksamheter är beroende av tillförlitlig och tillgänglig information och att den hanteras korrekt. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. När vi har en bra informationssäkerhet skapas förtroende för kommunen både inom och utanför våra verksamheter. Bristar i hantering av information leder omvänt till ett försämrat förtroende för kommunen hos både anställda, medborgare och andra samhällsaktörer. Bristar i informationssäkerhetsarbetet kan få katastrofala följder för såväl enskilda individer som hela verksamheter. Idag hanterar vi en allt större mängd information elektroniskt vilket ökar behovet av standardiserade modeller och tydliga rutiner för att upprätthålla informationssäkerheten.

Informationssäkerhet handlar om att ge information rätt skydd och omfattar:

**Konfidentialitet:** Att informationen skyddas mot obehörig insyn

**Riktighet:** Att informationen skyddas mot oönskad förändring

**Tillgänglighet:** Att information görs åtkomlig för behörig person vid rätt tillfälle

**Spårbarhet:** Att vi ska kunna kontrollera att informationen inte ändrats, eftersökts eller lämnats ut på ett felaktigt sätt eller till någon obehörig

### Vems ansvar?

Ansvaret för informationssäkerhetsarbetet följer det ordinarie verksamhetsansvaret. Detta gäller genomgående i den kommunala verksamheten, från ledning ner till enskilda medarbetare. En verksamhet kan bedrivas i en organisatorisk del som i t.ex. en avdelning, i löpande arbetsflöden och processer och även i ett tidsbegränsat arbete som t.ex. ett projekt. Det betyder att du som är verksamhetsansvarig ansvarar för att din verksamhet och dina anställda följer de policys som fastställs



i Överkalix kommun. Du som är anställd medarbetare vid Överkalix kommun, direkt eller via bolag, eller utför arbete åt entreprenör på uppdrag av Överkalix kommun, är skyldig att följa policyn och de riktlinjer, rutiner och instruktioner som tas fram.

## Med vems hjälp?

De personer som arbetar specifikt med informationssäkerhet har en viktig stödfunktion i sin organisation – ungefär på samma sätt som de personer som har stödfunktioner inom andra verksamhetsområden, som ekonomi, personal eller kommunikation. Du kan alltid vända dig till kommunens informationssäkerhetsansvariga för råd och stöd. I Överkalix kommun är detta säkerhetssamordnaren och IT-avdelningen.

## Mål

Med Policy för informationssäkerhet i Överkalix kommun ska vi snarast lägga grunden till ett starkt och medvetet skydd av den information vi arbetar med eller förvarar i kommunen. Vi ska aktivt arbeta för och ta ansvar för att den information vi handskas med är korrekt och tillgänglig för behöriga. Vi ska även aktivt arbeta för att förebygga händelser och handhavande av information som kan leda till negativa konsekvenser för vår informationssäkerhet. Det här innebär att vi fortlöpande analyserar och bedömer de system vi använder såväl som hur vi använder dem och att var och en ska vara uppmärksam på och rapportera händelser som kan misstänkas påverka informationssäkerheten.

Överkalix kommun ska eftersträva att följa Svensk Standard för Informationssäkerhet enligt ISO/IEC 27000-serien.

## Målgrupp

Policyn gäller för och i all verksamhet inom Överkalix kommun och dess bolag.

Samtliga anställda, såväl politiker som tjänstemän och extern personal omfattas av policyn och Överkalix kommuns riktlinjer och instruktioner för informationssäkerhet och informationshantering. Med information avses all information oavsett om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock, som ett samtal i korridoren eller i telefonen. Även film, ljud och bild omfattas av informationssäkerhetsbegreppet.

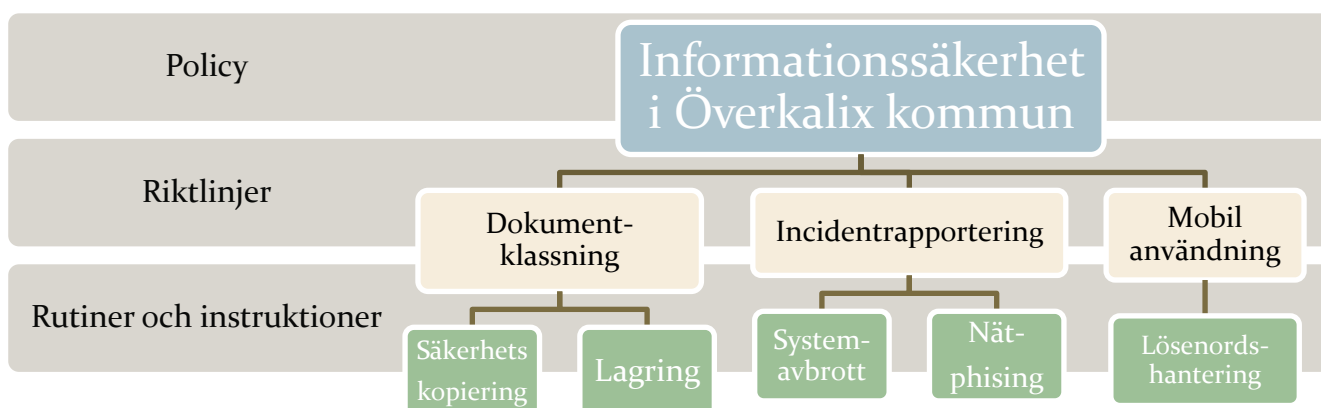
## Styrning av informationssäkerheten i Överkalix kommun

**Informationssäkerhetspolicy:** Avser ledningens viljeinriktning med informationssäkerhet.



**Riktlinjer:** Avser organisationsövergripande regler och rekommendationer, och kan innehålla både ska- och bör-krav.

**Instruktioner:** Avser vilka regler och rekommendationer som är specifika för en viss verksamhet, teknisk plattform eller situation. Kan även vara en fördjupning av en specifik riktlinje. Kan innehålla både ska- och bör-krav.



## Organisation, roller och ansvar

Genom att förtydliga organisation, roller och fördelning av ansvar säkerställer vi att IT-system och tjänster kan administreras och hanteras på ett sådant sätt att de under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål.

**Kommunfullmäktige** uttrycker sin viljeinriktning i denna policy.

**Kommunstyrelsen** har det yttersta ansvaret för kommunens informationssäkerhetsarbete.

**Kommundirektör** ansvarar för att tillse att kvalitets- och informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och genom att fördela resurser.

**Kommundirektör** (eller förvaltningschef) ansvarar för att systemägare utses.

**Varje chef** med personal eller verksamhetsansvar ansvarar för att det finns rutiner som säkerställer att anställda kan följa kommunens regelverk för informationssäkerhet.

**Informationssäkerhetssamordnaren** har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet.



**Informationsägarna** har ansvaret för informationen. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem. All information ska ha en informationsägare. Se följande tabell för exempel på vem som räknas som informationsägare om inget annat beslutats.

**Systemägarna** har ansvar för respektive system och dess användning. Systemen ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav. Systemen ska stödja informationens klassificering.

**Samtliga som hanterar informationstillgångar** har ett ansvar för att informationssäkerheten upprätthålls.

**Dataskyddsombud:** (tidigare personuppgiftsombud) I kommunen är styrelser, nämnder och förbund personuppgiftsansvariga. Enligt Dataskyddsförordningen ska de personuppgiftsansvariga utse dataskyddsombud med sakkunskap om lagstiftning och praxis om dataskydd. Rollen ska vara självständig, rådgivande och övervakande så att reglerna i Dataskyddsförordningen följs.

## Avtal och ansvarsfördelning

För att tydliggöra ansvar bör avtal upprättas som beskriver formell ansvarsfördelning. Servicenivåavtal ska upprättas mellan systemägare och intern eller extern tjänsteleverantör. Här skall behov av skydd och tillgänglighet beskrivas utifrån verksamhetens behov och den informationsklassning som gäller. I avtalen skall också metoder för mätning och uppföljning beskrivas.

Personuppgiftsbiträdesavtal ska finnas om någon part utanför den personuppgiftsansvariges egen organisation hanterar personuppgifter som ligger under dennes ansvar.

## Klassificering av information

Klassificering av information är en grundläggande aktivitet för att bedöma information och sedan kunna skydda och behandla den på rätt sätt utifrån dess informationsklass. All information ska därför klassificeras utifrån dess krav på konfidentialitet och sekretess, riktighet och tillgänglighet. All information som är personuppgifter eller relaterade till personuppgifter ska även klassas utifrån kraven på spårbarhet. Det ska förtecknas vilken klassificering en informationsmängd har. All hantering, bearbetning och lagring av information skall motsvara kraven i dess klassning.

## Hantering av avvikelser och undantag

Vi ska arbeta proaktivt för att förebygga att informationssäkerhetsincidenter inträffar. Om incidenter ändå inträffar ska skadorna minimeras så långt som det är möjligt genom tydliga riktlinjer och incidenthanteringsplaner.

Samtliga avvikelser ska dokumenteras och följas upp för att kontinuerligt förbättra vårt informationssäkerhetsarbete.

Informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning ska anmälas till ansvarig myndighet



ÖVERKALIX  
KOMMUN

## Uppföljning

Det åligger Kommunstyrelsen att minst en gång per år informera sig om hur arbetet med informationssäkerhet går. Kommunstyrelsen ska utifrån den årliga uppföljningen fatta beslut om åtgärder för att förbättra informationssäkerhetsarbetet samt tilldela nödvändiga resurser.

Postadress

956 81 ÖVERKALIX

Internet: [www.overkalix.se](http://www.overkalix.se)

Besöksadress

Storgatan 17

Telefon

0926-740 00

E-post: [kommun@overkalix.se](mailto:kommun@overkalix.se)

Telefax

0926-77920

Bankgiro

757-9311