
# Strategi för informationssäkerhet, cybersäkerhet och dataskydd

Diarienummer KS 25/76

Ånge kommun

**Mål** **Mål beskriver vad kommunen ska uppnå. Den är många gånger abstrakt och beskriver sällan sättet som det uppnås på. De kan innehålla långsiktiga perspektiv och beskriver verksamhetsområden som ska utvecklas och i vilken riktning.**
***Exempel på mål*: Mål och prioriteringar.**

**Plan** Kommunens mål omsätts till handling oftast genom en plan. De beskriver närmare hur verksamheten ska arbeta för att uppnå satta mål.
*Exempel på plan:* Verksamhetsplan.

**Riktlinje** Riktlinjer ska ge konkret stöd för hur arbetsuppgifterna ska utföras. De beskriver ramarna och riktningen för området. Riktlinjer ska vara så detaljerade att våra medarbetare ska känna sig trygg i sitt agerande, men utan att detaljstyra ageranden.
Exempel på riktlinje: Riktlinjer för styrdokument.

**Policy** En policy ska ge en princip att hålla sig till; ett sätt att se på en viss företeelse. En policy säger hur vi ska förhålla oss i t ex kommunikationsfrågor, hur vi ser på hemarbete eller hur kosten ska vara för de vi serverar.
*Exempel på policy:* Kommunikationspolicy

**Regel** Regler ska ge absoluta gränser för vårt agerande. Typiska ord och uttryck i sådana dokument är ”ska”, ”måste” och ”får inte”.
Exempel på regel: Regler för Ånge kommuns borgensåtagande.

| | |
|---|---|
| Omfattar | Koncernen |
| Dokumentansvarig | Stabschef |
| Fastställd av | Kommunstyrelsen |
| Fastställd när | (Datum och §§) |
| Giltig från och med | (ÅÅÅÅ-MM-DD) |
| Giltig till | (ÅÅÅÅ-MM-DD, max fyra år) |

Ånge kommun

# Innehåll

Ånge kommun

# 1 Bakgrund

Strategin är gemensam för Ånge kommun och Sundsvall kommun utifrån IT-samarbetet. Strategin utgår ifrån kommunens ledningssystem för informationssäkerhet och Sundsvalls kommuns strategi för en hållbar digital utveckling 2030.

Strategin beskriver på ett övergripande sätt syftet, förutsättningar och mål när det gäller informationssäkerhet, cybersäkerhet och dataskydd. Strategin beskriver också krav och principer samt hur den övergripande styrningen, planeringen och uppföljningen ska ske.

Strategin beskriver också hur den övergripande organisationen för arbetet med informationssäkerhet, cybersäkerhet och dataskydd är ordnad.

Strategin verkställs genom kommunernas verksamhetsplaner och följs årligen upp i respektive kommuns interna kontrollplaner.

# 2 Syfte och mål

Sundsvall och Ånge kommun ska säkerställa ett övergripande systematiskt informationssäkerhetsarbete som minskar risken för incidenter och skapar ett ökat förtroende för kommunernas tjänster i samhället. Digitaliseringen ska genomsyras av ett fokus på cybersäkerhet både i utvecklingen samt i den dagliga driften och i tillhandahållandet av digitala tjänster till kommunernas målgrupper.

Informationssäkerhet, cybersäkerhet och dataskydd ska ytterst bidra till att kommunerna kan leverera viktiga samhällsfunktioner och service som är säkra och värnar om den personliga integriteten.

Övergripande principer för arbetet med informationssäkerhet, cybersäkerhet och dataskydd är att:

- Utgå från att information är kommunens viktigaste tillgång och integrera systematiskt informationssäkerhetsarbete i våra verksamhetsprocesser
- Integrera systematiskt informationssäkerhetsarbete i våra verksamhetsprocesser för att möjliggöra en hållbar digitalisering
- Kompetens och förmågan inom informationssäkerhetsområdet ska utvecklas liksom förmågan att hantera informationssäkerhetsincidenter.
- Alla anställda ska ges tillräcklig kunskap om informationssäkerhet för att kunna inhämta, bearbeta och avlämna information inom ramen för de egna arbetsuppgifterna.
- En god säkerhetskultur ska genomsyra kommunerna. Med detta menas inte bara att medarbetarna har god kunskap om vilka säkerhetsregler som gäller utan att de också använder gott omdöme, samt kritiskt ifrågasätter och rapporterar händelser som kan påverka säkerheten.
- Säkerhetskraven för att förhindra olaga intrång ska vara höga främst på grund av den känsliga information som kommunerna hanterar. Säkerhetskraven ska verifieras genom återkommande intrångstester via oberoende extern part.
- Arbetet ska samordnas på övergripande nivå enligt den etablerade standardserien SS-ISO/IEC 27000 med målet att skapa och upprätthålla ett ledningssystem för informationssäkerhet (LIS).

Mer detaljerade mål för informationssäkerhet, cybersäkerhet och dataskydd beskrivs i kommunernas verksamhetsplan för informationssäkerhet, cybersäkerhet och dataskydd.

# 3 Roller och ansvar

Kommunernas nämnder och bolagsstyrelser har det yttersta ansvaret för informationssäkerheten. Grundprincipen att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret: Den som ansvarar för en viss verksamhet är också ansvarig för informationssäkerheten inom berört verksamhetsområde.

Högsta tjänsteperson i Sundsvall respektive Ånge har det yttersta ansvaret för att respektive kommun följer denna strategi. Högsta tjänsteperson ansvarar också för hanteringen av informationstillgångar och ska tillse att det finns resurser för detta.

Informationssäkerhetsansvarig (CISO) ansvarar för att säkerställa att arbetet med informationssäkerhet, cybersäkerhet och dataskydd sker i enlighet med tillämpliga interna och externa regelverk. CISO ansvarar för att erforderliga processer finns upprättade, för att kontroller, uppföljningar och rapporter hanteras löpande.

Ansvaret och uppgifter för CISO och för andra roller med särskilt ansvar för informationssäkerhet, cybersäkerhet och dataskydd finns beskrivna i kommunernas verksamhetsplan för informationssäkerhet, cybersäkerhet och dataskydd.

# 4 Informationssäkerhet, cybersäkerhet och dataskydd

Informationssäkerhet handlar om att skapa och upprätthålla rutiner för att skydda information utifrån fyra aspekter.

- **Konfidentialitet**: att information inte tillgängliggörs eller avslöjas till obehörig
- **Riktighet**: att information är korrekt, aktuell och fullständig
- **Tillgänglighet**: att information är åtkomlig och användbar när den behövs
- **Spårbarhet**: att i efterhand kunna härleda specifika händelser till objekt

## 4.1 Informationssäkerhet – säker informationshantering

Arbetet med informationssäkerhet ska genomsyra all kommunal verksamhet oavsett om det gäller digitalisering, skydd av personuppgifter, informationssäkerhet i samhällsviktiga verksamheter och tjänster eller utifrån ett säkerhetskyddsperspektiv. Informationssäkerhet handlar framför allt om att förhindra att information läcker, förvrängs och förstörs. Informationssäkerhet handlar om all data, oavsett form. Det innebär att inom informationssäkerhet är det primära syftet att skydda uppgifternas konfidentialitet, riktighet och tillgänglighet. Varje medarbetare har ett ansvar att medverka i informationssäkerhetsarbetet och vid hantering av personuppgifter.

Informationssäkerhetsarbetet innefattar bland annat att;

- aktivt arbeta med att identifiera risker och hantera säkerhetshot,
- genomföra insatser för att eliminera eller minimera risker/konsekvenser,
- genomföra säkerhetstestning och återställningstester,
- medverka i arbetet med att utarbeta kontinuitetsplaner,
- fastställa och kommunicera de informationssäkerhetskrav som gäller inom kommunen och
- genomföra utbildningsinsatser.
- följa det framtagna ledningssystemet för informationssäkerhet

## 4.2 Cybersäkerhet

Cybersäkerhet handlar om tekniker, metoder och processer för att skydda och försvara digitala tillgångar såsom datorer, servrar, mobila enheter, elektroniska system, nätverk och data från hot, skador, attacker eller obehörig åtkomst.

Inom cybersäkerhet är det primära syftet att skydda mot obehörig elektronisk åtkomst till data och att arbeta enligt ramverket; identifiera, skydda, upptäcka och återställa.

Cybersäkerhetsarbetet innefattar bland annat att;

- identifiera riskerna för cyberattacker
- utveckla en beredskapsplan för att hantera dessa cyberrisker och
- utbilda medarbetare i säkerhetsmedvetenhet.

Det ska finnas ett cybersäkerhetscenter som är en del av Sundsvalls kommuns kommunstyrelsekontor och organisatoriskt placerat under avdelningen för digitalisering och IT. Cybersäkerhetscentret samordnar och hanterar Sundsvall och Ånge kommuns cybersäkerhet.

## 4.3 Dataskydd

Kommunernas förvaltningar, bolag och förbund hanterar personuppgifter i stor mängd som ofta är känsliga ur ett integritetsperspektiv. Det är därför viktigt för kommunernas förtroende att organisationen arbetar aktivt med dataskydd.

Dataskyddsarbetet innefattar bland annat att:

- vid hantering av personuppgifter respekteras enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter
- personuppgifter samlas in och behandlas lagligt, rättvist och korrekt
- personuppgifter behandlas för uttryckliga och legitima syften
- enskilda informeras om hur hans/hennes personuppgifter hanteras
- personuppgifter är relevanta och nödvändiga för personuppgiftshanteringen och skyddas med ändamålsenliga organisatoriska och tekniska säkerhetsåtgärder

# 5 Uppföljning och rapportering

Uppföljning, kvalitetssäkring och dokumentation av arbetet ska ske återkommande och preciseras i planer som så långt som möjligt ska integreras i befintliga rutiner för planering och uppföljning av verksamheten. Uppföljning av kommunernas informationssäkerhetsarbete ska årligen rapporteras i kommunstyrelsen samt i förvaltningsledningarna.

I samband med uppföljningen redogörs bland annat för;

- trender inom området,
- status för arbetet,
- övergripande risker och
- incidenter

Informationssäkerhetsstrategin revideras var fjärde år. För detta ansvarar informationssäkerhetsansvarig inom kommunen.