Regler för Informationssäkerhet 2024–2026

Diarienummer KS 23/530

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	Kommunkoncernern
Dokumentansvarig	Informationssäkerhetssamordnaren
Fastställd av	Kommunstyrelsen
Fastställd när	2023-09-05, § 144
Giltig från och med	2024-01-01
Giltig till	2026-12-31

Ånge kommun

Innehåll

1 Kommunens syn på informationssäkerhet....1
2 Bakgrund....2
3 Grundläggande mål för informationssäkerhetsarbetet....3
4 Organisation, roller och ansvar....4
4.1 Organisation av informationssäkerhetsarbetet....4
5 Uppföljning....5

1 Kommunens syn på informationssäkerhet

Regler för informationssäkerhet är det övergripande dokumentet som styr kommunens informationssäkerhet.

Regler för informationssäkerhet redovisar kommunens viljeinriktning och stöd för Informationssäkerhetsarbetet och syftar till att klarlägga

- mål,
- organisation, ansvar och roller samt
- riktlinjer för områden av särskild betydelse

Informationssäkerhetsarbetet stödjer kommunens strategiska inriktning samt ingår som en del i kommunens process för ledning och styrning.

Information är en av kommunens mest strategiska resurser. Alla verksamheter är beroende av tillförlitlig information. Avbrott i tillgänglighet till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser för kommunens verksamhet eller tredje part.

Ledning och styrning av informationssäkerheten konkretiseras i ett ledningssystem för informationssäkerhet som säkerställer rätt nivå på informationssäkerhetsarbetet.

Kraven på informationssäkerheten utgår från kommunens och verksamhetens krav på funktion och tillämplighet liksom legala krav, förordningar, föreskrifter, avtal och säkerhetskrav. Med rätt informationssäkerhet uppnås hög kvalitet och god effektivitet i det dagliga arbetet.

Risken för störning ska minimeras samtidigt som skydd och åtgärd kontinuerligt balanseras mot kostnader. Insatser utgår från verksamhetens behov och är en del av kommunens totala riskhantering.

Kommunstyrelsen fastställer vilka system som är samhällsviktiga. Definitionen av samhällsviktiga system är den information som vid ett bortfall eller en svår störning kan leda till stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden. Dessa system ska genomgå en systemsäkerhetsanalys som utgör underlag för systemägares beslut om driftgodkännande.

Ånge kommun följer etablerade standarder och vägledningar för informationssäkerhet.

Dokumentet ska, av chef eller av denne utsedd person kommuniceras till samtliga anställda vid nyanställning samt när dokumentet är ny eller reviderad. Dokumentet ska vara känd och tillgänglig i aktuell version på kommunens Intranät och på kommunens hemsida.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i detta dokument.

2 Bakgrund

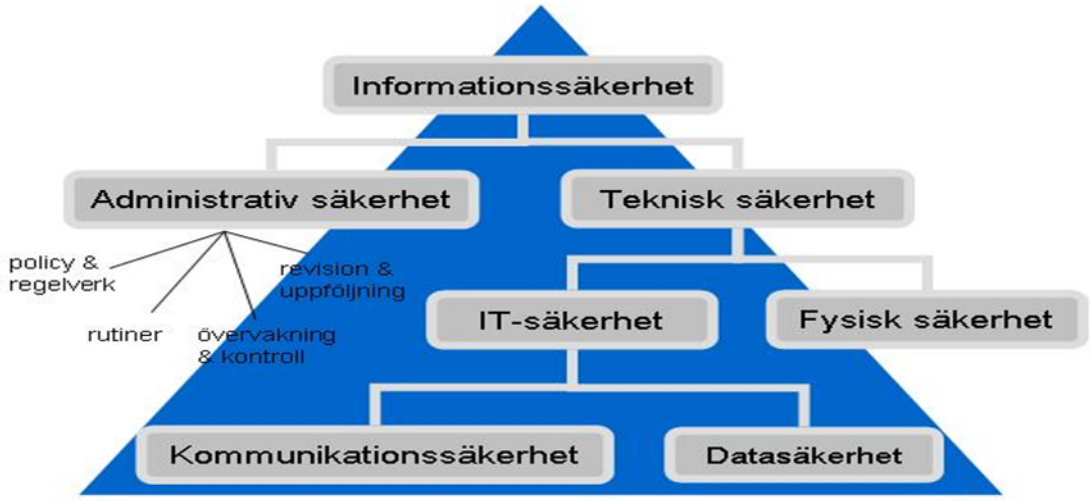
Kommunens alla verksamheter är beroende av att information är tillgänglig för rätt person vid rätt tidpunkt samt att den är korrekt och riktig samt utgör ett bra verksamhetsstöd. Det finns många hot mot våra informationstillgångar. För att säkerställa att informationen är skyddad finns det särskilda informationssäkerhetskrav som behöver uppfyllas.

Med informationssäkerhet avses skydd av informationstillgångar i syfte att upprätthålla nödvändig nivå på sekretess, riktighet, tillgänglighet och spårbarhet.

- Sekretess, att information skyddas för obehörig insyn
- Riktighet, att information är tillförlitlig, korrekt och fullständig
- Tillgänglighet, att information är nåbar vid rätt tillfälle
- Spårbarhet, att specifika aktiviteter som rör information kan spåras

Enkelt uttryckt kan informationssäkerhet delas upp i två delar. Den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. Den tekniska säkerheten är den delen som generellt beskrivs som IT-säkerhet. Här återfinns nätverk, servrar, arbetsstationer, hård- och mjukvara, serverrum och utrymme för reservkraft, samt fysisk säkerhet och säkerhet för personuppgifter (dataskydd).

Bilden nedan illustrerar skillnaden på administrativ och teknisk säkerhet.



Den tekniska säkerheten förutsätter att det finns en administrativ säkerhet för att rätt tekniska åtgärder ska kunna vidtas. IT-säkerhet är alltså endast en mindre del av informationssäkerhetsbegreppet.

3 Grundläggande mål för informationssäkerhetsarbetet

Ånge kommuns informationssäkerhetsarbete syftar till att uppfylla följande mål.

Medborgares och intressenters förtroende	• Informationssäkerhet ska bidra till att medborgare och andra intressenter ska känna sig trygga vid informationsutbyte med kommunen och vår förmåga att hantera känsliga personuppgifter.
Verksamhetens informations-säkerhet	• Samtliga anställda inom kommunens verksamheter ska ha kännedom och kunskap om aktuella regelverk beträffande informationssäkerhet. • Att grunden för ett systematiskt arbete resulterar i en god informationssäkerhet som är anpassad efter verksamhetens förutsättningar och behov. • Det systematiska informationssäkerhetsarbetet ska minst omfatta informationsklassning, hot- och riskanalys, incidenthantering, kontinuitetsplaner samt uppföljning, åtgärder och återkoppling. • Oväntade händelser i IT-systemen som kan leda till negativa konsekvenser ska minimeras och förebyggas. • Det ska finnas en kommunikationsplan som aktiveras vid händelser som har påverkan på informationssäkerheten. • Investeringar och information ska skyddas i paritet med dess värde med beaktande av de negativa konsekvenser som otillräcklig säkerhet kan medföra. • Det ska finnas dokumentation av samtliga IT-system
Författningar	• Att uppfylla de krav som ställs på informationssäkerheten i lagar, förordningar och föreskrifter.
Standarder	• Arbetet med informationssäkerhet ska följa etablerade standarder för informationssäkerhet.
Krishantering	• Hoten mot informationstillgångarna ska fortlöpande analyseras och informationssäkerheten ses som en del av kommunens

	krishanteringsplan, i syfte att stärka förmågan att driva verksamheten vidare i händelse av en kris.
Samhällsviktiga system	• Systemsäkerhetsanalyser ska genomföras • Hotbilden ska löpande analyseras och följas upp • Förebyggande åtgärder ska vidtagas • Kontrolleras så att krishanteringsförmågan upprätthålls • Allvarliga incidenter ska anmälas till tjänsteman i beredskap (TIB), säkerhetschef och informationssäkerhetsansvarig,

4 Organisation, roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att IT-system och tjänster kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetsreglernas mål.

All information ska klassificeras utifrån dess krav på Konfidentialitet (sekretess), riktighet, tillgänglighet och spårbarhet. Beroende på vilken klassificering som råder för en viss typ av information ska IT-system, tjänster, program och informationsmängder vara identifierade och förtecknade.

4.1 Organisation av informationssäkerhetsarbetet

- Kommunstyrelsen uttrycker sin viljeinriktning i detta regelverk.

- Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhetsarbete.

- Närmsta chef ansvarar för att det finns rutiner som säkerställer en god efterlevnad av kommunens regelverk för informationssäkerhet.

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

- Informationsägarna har det övergripande och yttersta ansvaret för informationen. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem.

- Systemägarna har övergripande ansvar för respektive system och dess användning. System ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav. Systemens informationsmängder ska klassificeras.

- Systemförvaltarna har det funktionella helhetsansvaret för ett system. Systemförvaltaren fungerar i hög grad som systemägarens utförare och ser till att systemets funktionalitet upprätthålls samt att planerade och beslutade aktiviteter genomförs i det dagliga arbetet.

- Alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls.

- IT-chefen eller motsvarande har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen.

- IT-chefen eller motsvarande har ett särskilt ansvar för den tekniska IT-säkerheten. Arbetar i nära samverkan med informationssäkerhetssamordnaren.
- IT-säkerhet är den miljö som faller under begreppet IT-infrastruktur.

- Informationssäkerhetsansvarig samordnar och planerar övergripande aktiviteter och är rådgivande till ledningen och kommunens förvaltningar

5 Uppföljning

Kommunstyrelsen/ledningen ska minst en gång per år informera sig om hur arbetet med informationssäkerhet går. Uppföljningen ska baseras på underlag med rekommendationer som tas fram av informationssäkerhetssamordnaren.

Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten
- Utbildning (status och behov)
- Inträffade incidenter av större påverkan på verksamheten.
- Resultat från genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till förbättringar

Resultatet från denna uppföljning ska innefatta beslut om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser.

Om misstanke om oegentlighet uppstår ska detta utan fördröjning anmälas till närmaste chef. I de fall regler inte följs kan följden bli disciplinära åtgärder. Om man kan förmoda att brott mot lag har begåtts lämnas information till brottsutredande myndighet.