

Informationssäkerhetspolicy för Ånge kommun

Denna informationssäkerhetspolicy anger hur Ånge kommun arbetar med informationssäkerhet och uttrycker kommunens stöd för och syn på informationssäkerhet.

Dokumentnamn Informationssäkerhetspolicy		Dokumenttyp Policy	Omfattar Ånge kommun
Dokumentägare Kommunchefen	Dokumentansvarig Informationssäkerhetssamordnaren	Publicering Intranät och internet	Informationsklass allmän
Fastställd KF 2017-11-27, § 91	Giltighetstid Uppföljning sker senast år 2023	Beslutsinstans Kommunfullmäktige	Diarienummer KS 17/270
Denna policy upphäver tidigare Informationssäkerhetspolicy KS 2009-02-04 § 14			

Ånge kommuns dokumentstruktur:

Politiska styrdokument:	Styrdokument – tjänstemannanivå:
<i>Reglemente</i>	
<i>Strategi</i>	
<i>Mål och prioriteringar, ekonomisk plan (Budgetdokumentet)</i>	
Policy	
<i>Plan, handlingsplan, åtgärdsplan</i>	<i>Plan, handlingsplan, åtgärdsplan</i>
<i>Politiska riktlinjer</i>	<i>Riktlinjer</i>
	<i>Rutiner</i>
	<i>Regler</i>
	<i>Instruktioner</i>

Innehållsförteckning

1	Kommunens syn på informationssäkerhet.....	4
2	Bakgrund	5
3	Omfattning.....	6
4	Grundläggande mål för informationssäkerhetsarbetet	6
5	Styrning av informationssäkerheten	8
6	Organisation, roller och ansvar	8
	6.1 Organisation av informationssäkerhetsarbetet.....	9
7	Uppföljning.....	10

1 Kommunens syn på informationssäkerhet

Informationssäkerhetspolicyn 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.

Policyn ska, av chef eller av denne utsedd person kommuniceras till samtliga anställda vid nyanställning samt när policyn är ny eller reviderad. Policyn 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 denna policy. Informationssäkerhetspolicyn ska fastställas i fullmäktige.

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.

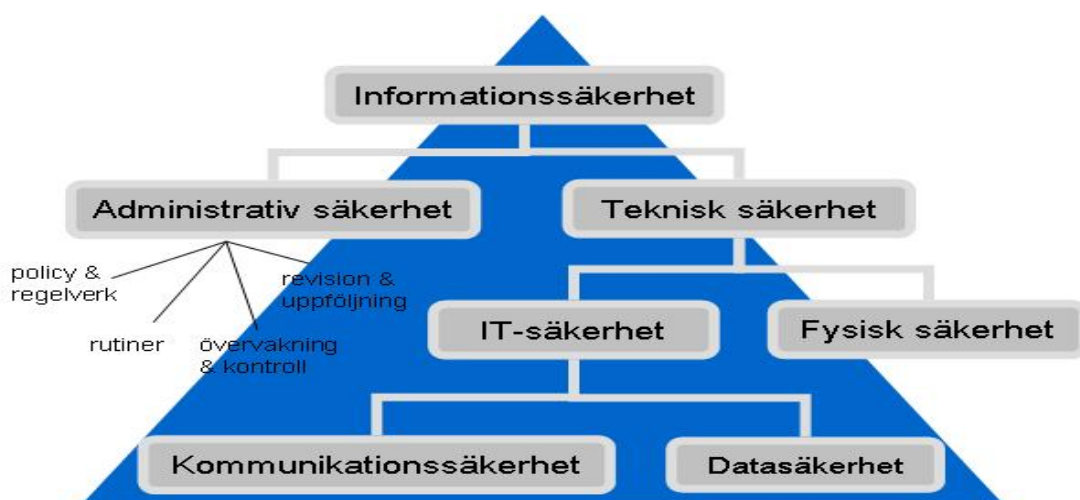
Det finns många hot mot våra informationstillgångar. För att säkerställa att informationen är skyddad finns det särskilda informationssäkerhetskrav som behöver uppfyllas.

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 samt serverrum och utrymme för reservkraft, säkerhetskopior etc.

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 Omfattning

Denna informationssäkerhetspolicy gäller för all verksamhet inom Ånge kommun, inklusive bolag.

Samtliga anställda, politiker och extern personal omfattas av policyn och dess tillhörande instruktioner.

Med informationstillgång 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.

Informationssäkerhet omfattar alla kommunens informationstillgångar.

4 Grundläggande mål för informationssäkerhetsarbetet

Ånge kommuns informationssäkerhetsarbete syftar till att uppfylla följande mål.

Medborgares och intressenters förtroende	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Samtliga anställda inom kommunens verksamheter ska ha kännedom och kunskap om aktuellt 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.

	<ul style="list-style-type: none">• Öväntade 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	<ul style="list-style-type: none">• Uppfylla de krav som ställs på informationssäkerheten i lagar, förordningar och föreskrifter.
Standarder	<ul style="list-style-type: none">• Arbetet med informationssäkerhet ska följa etablerade standarder för informationssäkerhet
Krishantering	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Obligatoriskt att systemsäkerhetsanalys 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)

5 Styrning av informationssäkerheten

Informationssäkerhetspolicyn är det övergripande dokumentet som styr kommunens informationssäkerhet. Policyn anger informationssäkerhetens betydelse för kommunen och motsvarar den översta delen i pyramiden. Ett exempel är att kommunen uttrycker att information ska vara tillgänglig och återläsningsbart.



Riktlinjerna beskriver vad som behöver göras för att efterleva informationssäkerhetspolicyn. Riktlinjerna motsvarar den mellersta nivån i pyramiden. Ett exempel på riktlinjer är t.ex. att säkerhetskopiering ska genomföras.

Baserat på riktlinjerna utformas instruktioner, rutiner och anvisningar som anger hur rutiner och säkerhetslösningar ska utformas och tillämpas. Detta motsvarar pyramidens lägsta nivå.

Den samlade dokumentationen tillsammans med de processer som ingår i ett systematiskt informationssäkerhetsarbete utgör ett ledningssystem för informationssäkerhet.

6 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 informationssäkerhetspolicyns 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.

Kommunchefen (i samråd med förvaltningschef) utser systemägare och informationsägare.

6.1 Organisation av informationssäkerhetsarbetet

- Kommunfullmäktige uttrycker sin viljeinriktning i denna policy.
- 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.
- Informationssäkerhetsråd eller motsvarande samordnar och planerar övergripande aktiviteter och är rådgivande till ledningen och kommunens förvaltningar

7 Uppföljning

Kommunstyrelsen/ledningen ska minst en gång per år informera sig om hur arbetet med informationssäkerhet går. Genomgången görs vid den årliga aktiviteten ”ledningens genomgång”.

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.