Systematiskt informationssäkerhetsarbete, policy

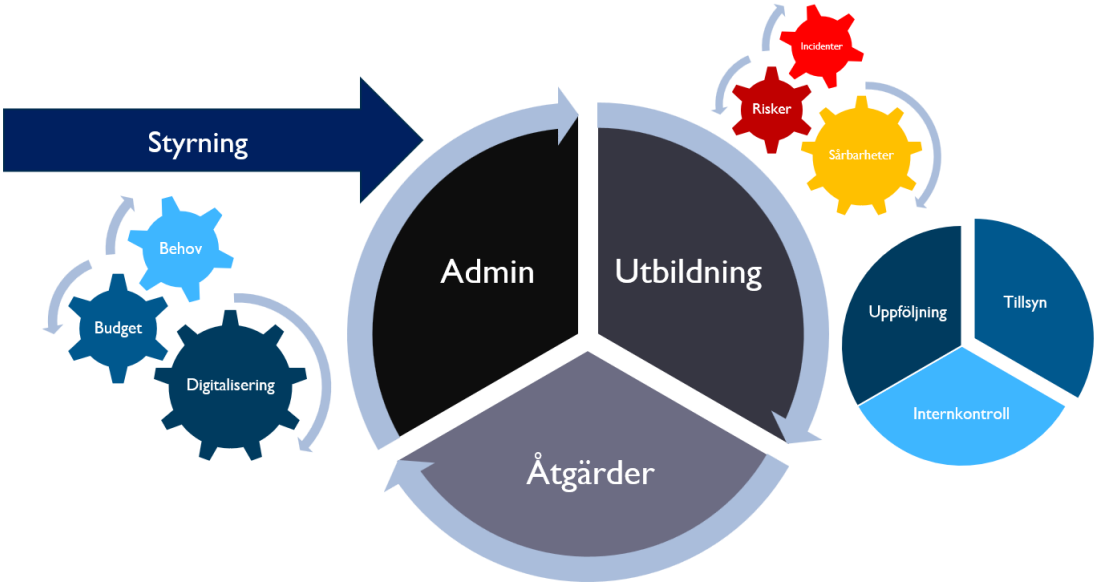
Dokumenttyp	Policy
Fastställd/upprättad	Kommunfullmäktige 2026-04-16, § 19
Senast reviderad	-
Detta dokument gäller för	Kommunövergripande
Giltighetstid	Tills vidare
Dokumentansvarig	Kommundirektör
Dnr	2026-89

Innehåll

Systematiskt informationssäkerhetsarbete

Det systematiska informationssäkerhetsarbetet ska vara närvarande i alla miljöer där Hjo kommun bedriver verksamhet och hanterar information av olika typer. Policyns innehåll baseras på bestämmelserna i Cybersäkerhetslag (2025:1506) och samordnar andra relaterade områden som styrs av bland annat Dataskyddsförordningen (GDPR/EU-direktiv) och Säkerhetsskyddslag (2018:585).

Syftet med det systematiska informationssäkerhetsarbetet är att all information, data och uppgifter hanteras på ett säkert sätt i kommunen. Säkerheten i informationshantering innefattar både tekniska åtgärder samt användarnas beteenden. Säkert innebär att arbetet är baserat på identifierade risker och att gällande lagar och föreskrifter följs. Information, system och tjänster för informationshantering ska alltid vara tillgängliga så att kärnverksamheten kan bedrivas samt informationen ska hållas riktig och skyddas från obehörig åtkomst.

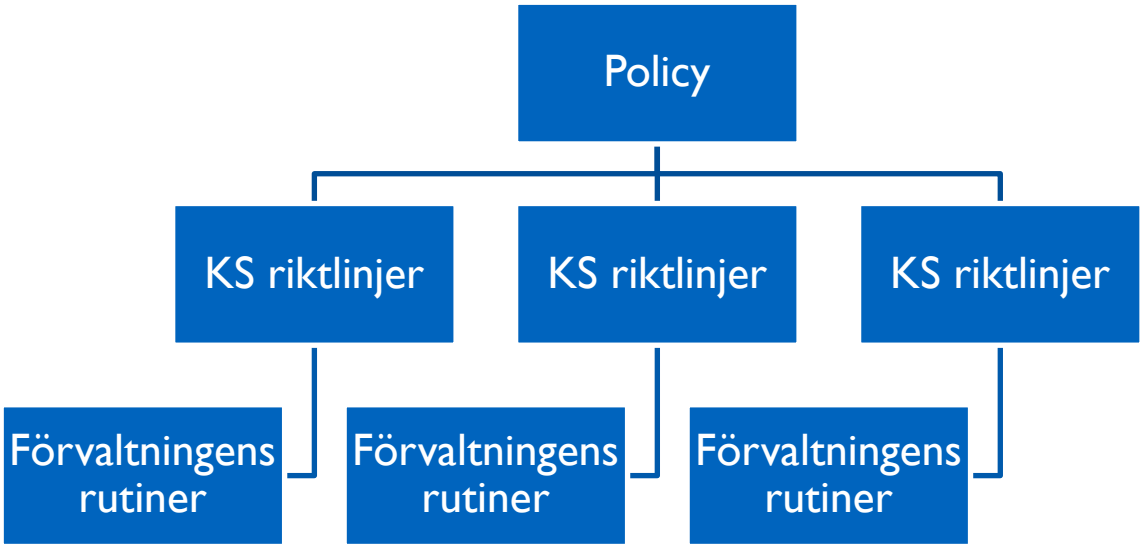


Figur 1 - Ett systematiskt informationssäkerhetsarbete inkluderar; styrning, administration, utbildning, förebyggande och underhållande åtgärder, avvikelse- och incidenthantering samt uppföljning och kontroll.

Ansvar och mandat

Kommunstyrelsen ska styra informationssäkerhetsarbetet genom riktlinjer eller motsvarande och vid behov vägleda och förtydliga utvalda delar för förvaltningen. Kommunstyrelsen ska årligen följa upp informationssäkerhetsarbetet och att denna policy följs. Inför innevarande mandatperiods slut ska slutsatserna från det genomförda arbetet redovisas till kommunfullmäktige.

Tillämpningen av bestämmelser gällande dataskydd enligt dataskyddsförordningen ska av byggnads- och valnämnden förtydligas vid behov men för kommunstyrelsen gäller det som åläggs nämnden i denna policy. Varje nämnd i kommunen är personuppgiftsansvarig för de personuppgifter som behandlas inom respektive verksamhetsområde. Nämnderna ska samverka i dataskyddsarbetet.



Figur 2 - Struktur över hur styrning av det systematiska informationssäkerhetsarbetet ska vara anordnat. Policyn styr ytterst. Kommunstyrelsen omsätter policyns innehåll till konkreta krav i riktlinjer och förvaltningen driver igenom inriktning och krav genom rutiner.

Inriktning för det systematiska arbetet

Hjo kommun ska följa nedan inriktning. Inriktningen ska vägleda det systematiska arbetet och ge ramar och vägledning för konkreta resultat.

Hjo kommun ska arbeta systematiskt, risk- och kunskapsbaserat samt resurs- och kostnadseffektivt med informationssäkerhet. Det innebär:

1. *Kommunen bör sträva efter att befintliga resurser nyttjas till maximal potential för arbetet.*
2. *Arbetet ska ledas av kommunledningen genom styrning, prioriteringar och inriktningar.*
3. *Alla ingående delar ska vara dokumenterade och arbetet ska vara förankrat i alla led i kommunens organisation.*
4. *Alla deltagare i arbetet ska ha relevanta kunskaper och färdigheter i syfte att bidra till en ökad säkerhet och effektivitet i arbetet.*
5. *Kostnader för arbetet ska kunna redovisas löpande.*

Uppföljning av arbetsområden

I slutet på varje mandatperiod ska arbetet enligt inriktningen presenteras för kommunstyrelsen i syfte att bereda revideringsbehov av denna policy inför nästkommande mandatperiod.

Nedan förtydligas hur det systematiska informationssäkerhetsarbetet i Hjo kommun bryts ner i respektive område som det består av. För alla områden gäller att information, system, verktyg, och data ska vara uppdaterade (riktighet), finnas tillhands när de behövs (tillgänglighet) och endast för de som har behov av dem och på annat sätt är behöriga (konfidentialitet). Alla informationstillgångar ska kunna spåras och kontrolleras för sin äkthet (autencitet).

Den inriktning som beslutats i denna policy ska vägleda och prioritera hur nedan områden ska

interagera med varandra. Inriktningen ska följas genom att kommunstyrelsen styr förvaltningen med tydliga anvisningar och ramverk för respektive område.

Informationssäkerhet

Informationssäkerhet är ett kommunövergripande arbete som ska bedrivas med fokus på beteenden hos all personal, politiker och andra som ges tillgång till kommunens information.

Information av olika typer bearbetas analogt, fysiskt, och digitalt i system och på IT-utrustning. Gränssnittet mellan dessa är inte alltid tydligt. Med anledning av det ska det finnas tydliga rutiner och förhållningssätt för alla målgrupper som denna policy omfattar och som berör all form av informationshantering, fysisk som digital.

Informationssäkerheten behöver vara sammanhållande för dataskydd, IT-säkerhet och systemförvaltning då alla dessa områden behandlar information.

Dataskydd

All personuppgiftshantering, oberoende eller i undantagsfall med stöd av eller hänsyn till annan lagstiftning, ska ske enligt dataskyddsförordningen, GDPR. Undantag meddelas av ansvariga myndigheter. Dataskydd kräver grundläggande informationssäkerhetsarbete, som tar hänsyn till beteenden hos den enskilde och till dataskyddsförordningens särskilda föreskrifter kring skyddet av de registrerades integritet. Dataskyddsarbetet behöver vara integrerat i det övergripande informationssäkerhetsarbetet.

IT-säkerhet och IT

Kommunens fysiska IT-miljöer måste vara utformade för att möta de risker som kan påverka dess funktionalitet och informationen i dem negativt. IT-säkerhetsarbetet i Hjo kommun bedrivs till stor del som inköpta tjänster från externa leverantörer för system och Skövde kommun för infrastrukturen och kräver regelbunden samverkan, samordning och kravställning samt uppföljning av vilka åtgärder som vidtagits av respektive leverantör. Det är avgörande att IT-säkerheten anpassas till de förutsättningar som finns i verksamheten och balanseras mellan risker, sårbarheter och kommunens övriga verksamhet. Användarvänlighet i den digitala miljön bidrar till ett säkert beteende.

Systemförvaltning

Kommunen har många olika system och digitala verktyg som nyttjas för att lösa diverse uppgifter. Dessa system hanterar nästintill all information som bearbetas i kommunens regi. Systemförvaltningen ska därav vara integrerat i kommunens systematiska informationssäkerhetsarbete i syfte att uppfylla kontinuitetskrav för kommunens digitala tjänster och system. Systemförvaltningen är kostnadsdrivande och ett bristande underhåll kan medföra stora kostnader. Höga kostnader leder till en sämre förmåga att vidta riskbaserade och förebyggande investeringsåtgärder i IT-säkerheten. Alla system och digitala tjänster som är avgörande för kommunens samhällsviktiga verksamhet behöver öva sin kontinuitet regelbundet.

IT

Drift och underhåll av IT-miljöer samt IT-utrustning gör det digitala arbetet möjligt. Det

innefattar uppföljning av kostnader, byte av utrustning samt regelbundet underhåll av hård- och mjukvara i alla miljöer. IT-arbetet är kopplat till användarvänligheten i utrustning genom att rätt typ tillhandahålls till rätt ändamål samt möjliggör tillgängligheten för användarna.

Digitalisering

Att digitalisera innebär att utveckla kommunens arbetsprocesser och verksamheter till en modern, effektiv och ändamålsenlig standard. Fokus ligger på förenkling, ökad tillgänglighet och säkrare hantering, vilket i sin tur leder till en bättre service till allmänheten. Digitalisering handlar även om utformningen av den digitala miljön såväl som användarnas förmåga, kreativitet och motivation att använda den till största effekt.

Riskhantering

Till grund för alla åtgärder, både organisatoriska och tekniska, ska identifierade risker ligga till grund. Syftet är att kostnaderna för arbetet ska motverka sårbarheter och risker som kan orsaka allvarliga konsekvenser för kommunens verksamheter.

Kommunen bör integrera informationssäkerhetsrisker i den övriga riskhanteringen och analysen av dessa bör relateras till andra risker som kommunen har identifierat. Informationssäkerhetsriskerna ska hållas uppdaterade och årligen ska riskerna omvärderas baserat på genomförde åtgärder och omständigheterna i övrigt.

Ekonomi

Alla kostnader som respektive område ovan orsakar kommunen ska vara redovisade och tillgängliga för granskning. Kommunstyrelsen ska styra hur dessa kostnader regelbundet ska redovisas.

Kommunstyrelsen ska styra hur och när anskaffningar av digitala tjänster, system eller infrastruktur ska ske och hur arbetet ska genomföras så att risker och sårbarheter förebyggs.

Artificiell intelligens

Många system och tjänster börjar nyttja artificiell intelligens, AI. Det ställer höga krav på kommunen att kunna avgöra om dessa AI-verktyg och system uppfyller gällande lag och förordning, och om nyttjande i övrigt är ändamålsenligt ur ett informationssäkerhets-, dataskydds- samt kostnadsperspektiv.

Politiker och anställda som nyttjar AI ska ha de kunskaper som krävs för att på ett säkert och effektivt sätt använda AI-verktyg. AI-användningen ska gynna arbetet och inte öka arbetsbördan.

Kommunstyrelsen ska styra vad AI får nyttjas till i kommunen genom att anta riktlinjer.

Utvecklingsarbete och digitalisering

Digitalisering är en utveckling av kommunens befintliga arbetssätt till en digital och effektivare form. Digitalisering ska leda till smidigare, tillgängligare och säkrare arbetssätt än de metoder som ersätts.

Digitalisering av kommunens verksamheter och processer ska ske med hänsyn till informationssäkerhet, dataskydd, IT-säkerhet, IT-driften och de ekonomiska förutsättningar som finns för den långsiktiga finansieringen av åtgärderna. Det är avgörande att digitaliseringen av kommunens verksamheter sker utifrån ett uttryckt och identifierat behov, snarare än en trendstyrd modernisering. Utvecklingen av digitala arbetssätt ska förbättra arbetsmiljön, göra Hjo kommun till en attraktiv arbetsplats och förbättra kvalitén i samt tillgängligheten av den service som levereras till allmänheten.

Kommunstyrelsen ska styra hur digitaliseringsarbetet ska ske och förtydliga vad som krävs för att uppfylla denna policy.

Beredskap och hantering vid incidenter

Hjo kommun ska ha beredskap att hantera incidenter och cyberattacker som stör verksamheten. Det innebär att verksamheten ska fortsätta att fungera även vid allvarliga IT-störningar eller avbrott i infrastruktur som IT är beroende av. Alla inträffade incidenter ska dokumenteras och vara underlag för riskanalys. Beredskapen för att hantera sådana avbrott ska övas i den omfattning som krävs, men minst årligen.

Kommunstyrelsen ska styra hur förvaltningen ska förebygga och hantera incidenter. Kommunstyrelsen ska även hållas uppdaterad över vilka incidenter som har inträffat, hur förvaltningen hanterat dessa och vad som görs för att reducera risken för förnyade incidenter.

Säkerhetsskydd och signalskydd

Information eller verksamhet som berör Sveriges säkerhet och därmed omfattas av bestämmelserna i säkerhetsskyddslagen ska samordnas med det systematiska informationssäkerhetsarbetet. Kommunen ska bedriva säkerhetsskydds- och signalskyddstjänst i enlighet med det identifierade behovet enligt gällande lagrum.

Deltagare i kommunens säkerhetskänsliga verksamhet ska vara säkerhetprövade i rätt nivå. Även ledamöter i kommunstyrelsen ska kunna säkerhetsprövas om förvaltningens säkerhetsskyddsanalys identifierat ett sådant behov. Omfattningen och nivå av sådana säkerhetsprövningar åligger kommunstyrelsen i samråd med kommundirektör samt säkerhetsskyddschef, att identifiera. Säkerhetsprövningar ska om möjligt ske innan en ledamot påbörjar sitt uppdrag i styrelsen.

Alla säkerhetsprövade befattningar ska ha kunskaper i informationssäkerhetens grunder och ges kompletterade utbildning och repetition i säkerhetsskydd regelbundet. Kommunstyrelsen ska styra kommunens säkerhetsskydds- och signalskyddsarbete så att förvaltningen vägleds att följa säkerhetsskyddslagen och andra tillämpbara författningar. Incidenter och slutsatser i säkerhetsskyddsarbetet ska redovisas i den årliga redovisningen till kommunstyrelsen.