

Handläggare:
IT-Chef, Stefan Ryman

Mottagare: Kommunfullmäktige

Skinnskattebergs kommuns informationssäkerhetspolicy

Antagen av Kommunfullmäktige 2025-06-09 § 77



Styrdokument i en kommun är viktiga verktyg som fastställer regler, riktlinjer och principer för hur kommunen ska styras och hur dess verksamhet ska bedrivas. Dessa dokument säkerställer en konsekvent och effektiv förvaltning samt främjar transparens och rättssäkerhet. Här är några vanliga typer av styrdokument i en kommun och deras funktioner:

1. Övergripande policyer

- **Verksamhetspolicy:** Definierar kommunens övergripande mål, vision och värderingar. Den fungerar som en vägledande ram för hur kommunen ska uppfylla sina uppdrag.
- **Miljöpolicy:** Styr arbetet med hållbar utveckling och miljöfrågor i kommunen.

2. Reglementen och riktlinjer

- **Reglementen:** Dessa dokument reglerar ansvarsområden och befogenheter för olika nämnder, styrelser och tjänstemän i kommunen, vilket säkerställer en tydlig och rättvis styrning.
- **Delegationsordning:** Anger vilka beslut som kan fattas av olika funktioner eller tjänstemän utan att behöva gå genom nämnder eller styrelser, vilket gör beslutsprocesser smidigare.

3. Strategidokument

- **Utvecklingsstrategier:** Exempelvis kan en **digitaliseringsstrategi** eller **utvecklingsplan för infrastruktur** ange långsiktiga mål och prioriteringar för kommunens utveckling inom specifika områden.
- **Budgetdokument:** Det ekonomiska styrdokumentet som definierar hur resurser ska fördelas och prioriteras inom kommunens olika verksamhetsområden.

4. Riktlinjer och rutiner

- **Personal- och arbetsmiljöriktlinjer:** Fastställer regler för hur arbetsmiljö, rekrytering och kompetensutveckling ska hanteras.
- **Informationssäkerhetsriktlinjer:** Beskriver hur kommunen ska skydda sin information och data, inklusive hantering av personuppgifter och digital säkerhet.

5. Planer och program

- **Översiktsplan:** En långsiktig plan för hur kommunen ska använda mark och vatten, och hur bebyggelse ska utvecklas.
- **Krisplaner:** Definierar åtgärder och beredskap vid krissituationer såsom naturkatastrofer eller tekniska haverier.

Sammanfattningsvis hjälper styrdokument en kommun att skapa struktur och tydlighet, säkerställer att verksamheten bedrivs på ett lagligt och korrekt sätt, och att man uppfyller både interna mål och externa krav från exempelvis staten och medborgarna

Beslutad av: Kommunfullmäktige

Datum: 2025-x-x

Innehållsförteckning

INLEDNING	3
Om denna informationssäkerhetspolicy	3
Om informationssäkerhet	3
INFORMATIONSSÄKERHETSMÅL	4
Långsiktiga mål (3-5 år, strategiska)	4
Kortsiktiga mål (1-2 år, mätbara)	4
PRINCIPER OCH ARBETSSÄTT	5
VERKSAMHETSDRIVEN INFORMATIONSSÄKERHET GENOM INFORMATIONSKLASSNING	6
ROLLER OCH ANSVAR	7
UPPFÖLJNING OCH RAPPORTERING	9

Inledning

Om denna informationssäkerhetspolicy

Denna informationssäkerhetspolicy gäller för Skinskattebergs kommun, och kompletterar våra övriga styrdokument inom bland annat IT, kvalitet, kommunikation och övrig säkerhet. Alla våra verksamheter omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna.

Informationssäkerhetspolicyn är ett övergripande dokument som redovisar Skinskattebergs kommuns övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat. Styrdokumentet Riktlinjer för informationssäkerhet är mer detaljerat och konkretiserar denna informationssäkerhetspolicy.

Om informationssäkerhet

Information finns i alla våra verksamheter och handlar om allt det vi gör, exempelvis om personal, tjänster, ekonomi och omvärld med kunder, leverantörer och andra aktörer. Information är därför i sig en av de viktigaste tillgångar.

För att nå en hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån tre 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 av behörig

Information har i olika grad krav på sig gällande de tre ovan aspekterna. Kraven kan härledas från rättsliga krav eller från Skinskattebergs kommuns egna målsättningar. Dessutom har kunder, leverantörer, och andra aktörer i vår omvärld, behov och förväntningar som ställer krav på vår informationssäkerhet.

Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller direkt av oss människor i form av tal.

Informationssäkerhetsmål

Skinnskattebergs kommun ska uppnå och upprätthålla en informationssäkerhet som är indelade i långsiktiga och kortsiktiga mål. Målen har syfte att uttrycka en viljeriktning med det interna informationssäkerhets- och dataskyddsarbetet och vara konkreta och ha en koppling till de brister som identifierats inom verksamheten.

Långsiktiga mål (3-5 år, strategiska)

- Alla kritiska informationstillgångar ska vara klassade och erhålla motsvarande skydd
- Informationssäkerheten bidrar till att verksamhetens uppsatta mål gällande exempelvis kvalitet, effektivitet och dataskydd uppnås
- Bidra till att lyfta medvetandet kring informationssäkerhet inom kommunen
- Upprätthålla invånarnas förtroende för kommunens informationshantering

Kortsiktiga mål (1-2 år, mätbara)

- Inrätta en säkerhetssamordnare.
- Inrätta rollen som informationssäkerhetsansvarig
- Implementera klassnings- och riskprocesser i organisationen
- Etablera process för incidenter och följa upp incidenter
- Genomföra medvetandehöjande insatser exempelvis utbildning
- Skapa robusta processer för personuppgiftshantering
- Etablera process för internrevision och granskning av informationssäkerhetsarbetet

Principer och arbetssätt

Skinskattebergs kommun ska arbeta med informationssäkerhet på ett sätt så att formulerade mål uppfylls. Arbetet med informationssäkerhet ska vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Skinskattebergs kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar riskerna till en acceptabel nivå.

Arbetet med informationssäkerhet inom Skinskattebergs kommun ska:

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 med målet att skapa ett ledningssystem för informationssäkerhet (LIS),
- löpande ses över och förbättras, eftersom Skinskattebergs kommun och vår omvärld, inklusive hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Skinskattebergs kommuns värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet.

Verksamhetsdriven informationssäkerhet genom informationsklassning

Verksamheter ansvarar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheter utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen, exempelvis vår IT-avdelning och externa systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Skinnskattebergs kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Roller och Ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från ledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Informationssäkerhetsansvarig och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till våra verksamheter att fullfölja informationssäkerhetsansvaret.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i riktlinjer för informationssäkerhet.

Medarbetare har ett ansvar att följa Skinnskattebergs kommuns informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Man har som medarbetare också ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerheten och meddela sådana skyndsamt till närmsta chef.

Kommunstyrelsen har det yttersta ansvaret för informationssäkerheten i kommunen.

Nämnden har det yttersta ansvaret för informationssäkerheten inom respektive verksamhetsområde.

Informationssäkerhetsansvarig har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig ska arbeta i samråd med övriga verksamheten. Funktionen finns inte i dag men skall inrättas (Bör ligga under kommunchef).

Informationssäkerhetssamordnare stöttar verksamheten operativt och samordnar arbetet med att uppnå informationssäkerhetspolicyns mål enligt ledningssystemet. Informationssäkerhetssamordnare ska bistå och stötta informationsägare vid utredning av informationssäkerhetsincidenter som faller inom informationsägarans ansvar samt följa upp och säkerställa samtliga informationssäkerhetsincidenters utredning och åtgärdshantering. Funktionen skall finnas i varje verksamhet.

IT-chef samordnar arbetet med säkerheten i vår IT- miljö. IT-chef har tillsynsansvar för att IT-miljön är tillförlitlig och motsvarar interna och externa krav.

Säkerhetsskyddschef ansvarar för kommunens arbete inom säkerhetsskyddsområdet.

Säkerhetssamordnare samordnar arbetet med den fysiska säkerheten. Funktionen finns inte på kommunen

Informationsägare ansvarar för att informationssäkerhetspolicy och riktlinjer för informationssäkerhet efterlevs inom dess verksamhetsområde. En viktig del i ansvaret är att besluta om objektets informationssäkerhetsnivå(-er) genom att klassning sker i enlighet med Skinnskattebergs kommuns modell för informationsklassning. Varje informationstillgång ska tilldelas en informationsägare med uppdrag att hantera alla delar av de krav som ställs på informationen. Informationsägare ska utse informationsförvaltare.

Informationsförvaltare har det operativa ansvaret för att upprätthålla alla delar av de krav som ställs på informationen för de informationstillgångar som informationsägaren ansvarar för.

Systemägare ansvarar för respektive IT-systems säkerhet och ansvarar även för framtagande av kontinuitetsplaner för systemet. Systemägare ansvarar för att hantering av information i organisationens IT-system möter de krav som ledningssystemet och informationsägare ställer. Systemägaren tillsätter systemförvaltare.

Systemförvaltare är den som vet hur man jobbar i systemet, som kan svara på frågor gällande hur systemet fungerar och har tillsammans med informationsägaren möjlighet att säkerhetsställa att information hanteras på rätt sätt i IT-systemet som systemägaren har ägarskap av.

IT ansvarar för att säkerheten i vår IT- miljö som tjänster, processer, system, infrastruktur, verktyg etc. är tillräcklig och uppfyller verksamheternas krav, legala krav samt denna informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet.

Personuppgiftsansvariga utses av kommunstyrelsen och de ansvarar för hanteringen av personuppgifter och ska utse dataskyddsombud som kontrollerar att personuppgifter hanteras på ett korrekt sätt i verksamheten.

Dataskyddsombudet har en samordningsfunktion när det gäller behandling, revidering och tillsyn av personuppgifter i hela kommunen.

Dataskyddssamordnare stöttar verksamheten operativt och samordnar arbetet med verksamhetens dataskydd. Dataskyddssamordnare ska bistå och stötta personuppgiftsansvariga vid utredning av personuppgiftsincidenter som faller inom den personuppgiftsansvariges ansvar samt följa upp och säkerställa samtliga personuppgiftsincidenters utredning och åtgärdshantering. Funktionen finns på varje kontor.

Uppföljning och rapportering

Efterlevnaden av informationssäkerhetspolicyn och riktlinjer för informationssäkerhet ska följas upp regelbundet.

Informationssäkerhetsansvarig ska årligen rapportera läge och status gällande informationssäkerhet till ledningen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.