



SVENLJUNGA  
KOMMUN

# policy

---

## Informationssäkerhet, Cybersäkerhet och dataskyddspolicy

---

Beslutat av	Kommunfullmäktige
Beslutandedatum	2025-06-16 § 70
Ansvarig	Kommunchef
Revideras	Vid behov
Följas upp	Årligen

---



# Innehållsförteckning

Inledning .....	3
Bakgrund .....	4
Informationssäkerhetens fyra delar .....	4
Personuppgiftshantering .....	5
Omfattning och principer.....	5
Riskhantering och säkerhetsstrategi.....	5
Incidenthantering.....	6
Ledningssystem för informationssäkerhet (LISD) .....	7
Organisation, roller och ansvar.....	7
Uppföljning.....	8

## Inledning

Denna policy redovisar Svenljunga kommuns viljeinriktning och övergripande principer avseende informationssäkerhet, cybersäkerhet och dataskydd i kommunen. Policyn konkretiseras i styrdokumentet *Riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd*. Syftet med policyn är att klarlägga:

- Mål
- Organisation, ansvar och roller
- Riktlinjer för områden av särskild betydelse

Information utgör en av de mest strategiska resurserna kommunen besitter. Alla verksamheter är beroende av tillförlitlig information där avbrott i tillgängligheten kan rendera i allvarliga konsekvenser för invånare, verksamheter och tredje part.

Kraven på informationssäkerhet utgår från kommunledningen och verksamhetens krav på funktion, tillämplighet och legala krav. Därutöver även avtal och säkerhetskrav. Med adekvat och rätt informationssäkerhet kan en hög kvalitet och god effektivitet uppnås i det dagliga arbetet. Det förebygger störningar, skapar kontinuitet och föreslår adekvata åtgärder mot de risker som identifieras. Insatser utgår från verksamheternas behov och ska vara en del av kommunens totala riskhantering.

Kommunledningsgruppen fastställer vilka verksamhetsprocesser som är samhällsviktiga. Den information och de IT-system som stöder de informationsflödena ska sålunda också betraktas som samhällsviktiga. Det medföljer en informationsklassning, risk-och sårbarhetsanalys och kontinuitetshantering som ska mynna ut och motsvara ett skydd som adresserar informationen och systemet som behandlas.

Oavsett om informationen behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i ska informationstillgångarna ha rätt skydd.

Kommunen ska i den utsträckning det är möjligt följa etablerade standarder och vägledningar som baseras på Svensk Standard för Informationssäkerhet i enlighet med ISO/IEC 27000-serien.

Policyn ska, av chef eller motsvarande, kommuniceras till samtliga anställda vid nyanställning samt när policyn är ny eller reviderad. Policyn ska vara känd och tillgänglig i aktuell version på kommunens Medarbetarwebb och på kommunens webbplats.

Avtal och överenskommelser får inte skrivas som åsidosätter kraven i denna policy.

## Bakgrund

Information finns och hanteras i alla kommunens verksamheter som är beroende av att information är tillgänglig för rätt person vid rätt tidpunkt, att den är korrekt och riktig och således utgör ett bra verksamhetsstöd och för att vi som organisationen ska kunna fullgöra vårt uppdrag i samhället.

Det finns idag många hot mot våra informationstillgångar och för att säkerställa att informationen är skyddad finns det särskilda informationssäkerhetskrav som behöver uppfyllas. Informationssäkerhet avgränsas till skydd av informationstillgångar och tar sikte på nödvändig och adekvat nivå på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

- Tillgänglighet: åtkomlighet för behörig person vid rätt tillfälle.
- Spårbarhet: härledning av utförda aktiviteter till en identifierad användare.
- Konfidentialitet: att information inte tillgängliggörs eller avslöjas till obehörig.
- Riktighet: att information är korrekt, aktuell och fullständig.

Informationssäkerheten omfattar skyddet av information oavsett form medan cybersäkerheten tar sikte på de hot, sårbarheter och skyddsåtgärder som rör den digitala miljön. Cybersäkerheten kan således tolkas som ett medel för att uppnå informationssäkerhetens mål i den digitala kontexten.

## Informationssäkerhetens grundpelare

En del av kraven kretsar kring medarbetares kunskap och vår organisationskultur kring informationssäkerhet. Det inbegriper utbildningar, övningar, processer och mallar med flera för våra verksamheter. Den delen kan betraktas som den mjuka delen i informationssäkerheten och ställer krav på organisationens chefer, att medarbetare ska genomföra utbildningar, följa gemensamma processer eller dylikt.

Den del som kan betraktas som den administrativa säkerheten består av styrning, organisation, roller och ansvar, liksom regelverk, processer och systematik. En viktig del är också revision och uppföljning.

Den tekniska säkerheten kan betraktas som den hårda delen och beskrivs också som IT-säkerhet. Häri återfinns nätverk, servrar, arbetsstationer, hård-och mjukvara samt serverrum. Här finns även reservkraft, säkerhetskopior med mera.

Den sista delen är fysisk säkerhet som till stor del hör ihop med den tekniska säkerheten. Den tar sikte på hur vi skyddar vår organisations materiel, system och personal rent fysiskt.

## Personuppgiftshantering

I många avseenden förekommer även personuppgifter i information som hanteras. Personuppgifter står under särskilt skydd och råder under särskilda bestämmelser enligt Dataskyddsförordningen (mer känd som GDPR) samt nationell kompletterande lag; Dataskyddslagen. För personuppgifter gäller således särskilda regler för hantering. Inom ramen för informationssäkerhet är det viktigt att identifiera personuppgifter som särskilt skyddsvärda samt ändamålsenligt hanterade.

## Omfattning och principer

Policyn är normerande, stödjande och kontrollerande och gäller all verksamhet inom Svenljunga kommun och omfattar alla informationstillgångar som kommunen hanterar.

Den innebär att samtliga anställda, förtroendevalda, elever och inhyrd personal omfattas av policyn och dess tillhörande rutiner. Ergo, den gäller för alla som brukar kommunens informationstillgångar på ett sådant sätt att de kan påverka informationens konfidentialitet, riktighet, och/eller tillgänglighet.

Informationstillgång definieras som all information, oaktat om den behandlas i ett IT-system, förekommer på ett utskrivet papper, i ett anteckningsblock som i ett samtal. Film, ljud och bild omfattas också av informationssäkerhetsbegreppet.

Det övergripande målet är enkelt uttryckt att rätt information ska vara tillgänglig för rätt person i rätt tid. Mer detaljer återfinns i *riktlinjerna*.

## Riskhantering och säkerhetsstrategi

Kommunen har en övergripande säkerhetsstrategi som utgår från en allriskansats och omfattar systematisk riskidentifiering, riskbedömning och riskhantering. Denna strategi är en central del av det systematiska informations- och cybersäkerhetsarbetet och är utformad i enlighet med kraven i NIS-2-direktivet (Cybersäkerhetslagen), Dataskyddsförordningen (GDPR), CER-direktivet och annan relevant lagstiftning.

Syftet med strategin är att stärka organisationens förmåga att förebygga, motstå, hantera och återhämta sig från incidenter som kan påverka

informationssäkerheten, kontinuiteten i samhällsviktiga tjänster och skyddet av personuppgifter. Riskhantering sker kontinuerligt, integrerat i verksamhetsstyrningen och inom ramen för de mandat som respektive förvaltning besitter. Att utifrån sin roll som informationsägare, bedöma och dokumentera vilka risker som kan accepteras inom respektive verksamhetsområde, med beaktande av lagkrav, skyddsvärden och den potentiella påverkan på andra delar av organisationen.

För att säkerställa enhetlighet och spårbarhet ska riskaccept dokumenteras på ett sätt som möjliggör granskning. Om en identifierad risk bedöms kunna påverka andra verksamhetsområden, gemensamma resurser eller kommunens samlade förmåga att leverera samhällsviktiga tjänster, ska bedömningen ske i dialog med ISCG och, vid behov, föras vidare till kommunövergripande ledningsnivå för vidare ställningstagande.

Mer detaljerad beskrivning av arbetssätt, roller och ansvar återfinns i tillhörande *riktlinjer*.

## Incidenthantering

I kommunen finns det en dokumenterad process för hantering av informationssäkerhets- och personuppgiftsincidenter. Syftet är att möjliggöra tidig upptäckt, korrekt rapportering, effektiv hantering och lärande efter incident.

Processen omfattar bland annat:

- Intern rapportering till ICSG (Information och cybersäkerhetsgruppen) informationssäkerhetssamordnare (CISO), IT-driftsledare och eventuellt dataskyddsombud.
- Bedömning av incidentens allvarlighetsgrad och påverkan.
- Rapportering till tillsynsmyndighet vid allvarliga incidenter i enlighet med NIS-2 (Cybersäkerhetslagen) (inom 24 timmar) och GDPR (inom 72 timmar).
- Återställning av verksamhet och informationssystem.
- Dokumentation, analys och förbättringsåtgärder.

Granulärare instruktioner och anvisningar återfinns i kommunens *riktlinjer*.

## Ledningssystem för informationssäkerhet (LISD)

Den samlade dokumentationen ihop med de processer som ingår i ett systematiskt informationssäkerhetsarbete utgör ett ledningssystem för informationssäkerhet, cybersäkerhet och dataskydd (LISD). Ledningssystemet bygger på standarden för ledningssystem för informationssäkerhet ISO/IEC 27001.

## Organisation, roller och ansvar

Organisation, roller och fördelning av ansvar ska säkerställa att information och tjänster kan administreras och hanteras på ett sådant sätt att de under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla informationssäkerhetspolicyns mål.

All information ska klassificeras utifrån verksamhetens krav på konfidentialitet, riktighet och tillgänglighet. Det ska förtecknas vilken klassificering en informationsmängd har. All hantering, bearbetning och lagring av information skall motsvara kraven i dess klassning.

Kommunfullmäktige är ytterst ansvarig för informationssäkerhets, cybersäkerhet och dataskyddsarbetet och uttrycker sin viljeinriktning i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhet, cybersäkerhet och dataskyddsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd.

Nämnder med förvaltning och kommunala bolag ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras.

Dataskyddsförordningens stadgar pekar ut att ansvaret är knutet till den som är personuppgiftsansvarig. Det innebär att det är kommunens nämnder som har det yttersta ansvaret för att personuppgiftsbehandlingar i varje enskilt fall utförs i enlighet med förordningens regler och principer.

Policyn för informationssäkerhet, cybersäkerhet och dataskydd gäller för alla informationstillgångar och personuppgiftsbehandlingar i alla verksamheter inom kommunen. Policyn gäller för samtliga aktörer som kan komma att hantera kommunens information och personuppgifter.

De som hanterar information och personuppgifter ska ha kunskap om det regelverk som gäller för hur informationen och personuppgifterna får hanteras och har själva

ett ansvar för att informationssäkerheten och dataskyddet upprätthålls. Vid upptäckt av incident eller brister ska incidentrapportering ske enligt rutin.

Andra termer av relevans är systemägare, objektägare, informationsägare och systemförvaltare. I regel är det informationsägare som också är riskägare, det vill säga den part som ansvarar för riskerna som identifieras i en risk-och sårbarhetsanalys.

## Uppföljning

Kommunstyrelsen och verksamhetsledningen ska minst en gång per år informera sig om arbetet med informationssäkerhet och arbetet som behandlas av denna policy. Denna uppföljning ska baseras på underlag med rekommendationer som tas fram av informationssäkerhetssamordnaren/CISO. Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten
- Utbildning (status och behov)
- Inträffade incidenter
- Resultat från genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till förbättringar
- Genomförda riskanalyser

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

Uppföljning ska årligen genomföras för att kontrollera att tekniken fungerar utifrån de säkerhetskrav som finns, samt att regler efterlevs. Ansvarig för uppföljningen är kommunens informationssäkerhetssamordnare. Genomförandet kan delegeras.

Ifall misstanke om oegentlighet uppstår ska detta utan fördröjning anmälas till närmsta 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.