Policy för informationssäkerhet

En digitaliserad värld förutsätter en tillförlitlig informationshantering

Beslutsinstans	Kommunfullmäktige
Beslutad	2022-03-29
Senast reviderad	Välj datum
Giltig till	Tills vidare
Dokumentansvarig	It-chef
Diarienummer	KS.2021.179

GNESTA KOMMUN

Innehållsförteckning

Policy för informationssäkerhet

All information vi hanterar är värdefull, både för oss som kommun och för den enskilde. Om information går förlorad eller är felaktig kan det få katastrofala följder och medföra stora ekonomiska förluster. Information är därför en av Gnesta kommuns viktigaste tillgångar.

Policyn för informationssäkerhet redovisar Gnesta kommuns övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat. Till policyn hör även riktlinjer. Alla verksamheter i kommunen omfattas av policyn, och det är inte tillåtet att besluta om lokala regler som avviker från riktlinjerna.

Syftet med informationspolicyn är att invånare, företagare, organisationer och övriga intressenter ska känna sig trygga i kontakten med Gnesta kommun och vara säkra på att personuppgifter och andra informationstillgångar hanteras på ett tillförlitligt sätt.

Policyn för informationssäkerhet är fastställd av kommunfullmäktige och gäller samtliga nämnder i Gnesta kommun från och med 2021-11-25.

Vad är informationssäkerhet?

Informationssäkerhet handlar om att skydda informationstillgångar som Gnesta kommun hanterar. Med informationstillgång menas allt som innehåller eller bär på information, som exempelvis text, ljud, bild och film. Detta oavsett hur informationen lagras, bearbetas eller kommuniceras. Det kan vara med stöd av system, datorer, mobiltelefoner, papper eller direkt av oss människor i form av tal.
Informationssäkerhet handlar om att skydda information utifrån tre aspekter:

- **Konfidentialitet**: att information inte görs tillgänglig eller avslöjas till obehörig.
- **Riktighet**: att information är korrekt, aktuell och fullständig.
- **Tillgänglighet**: att information är åtkomlig och användbar av behörig.

Arbetet med informationssäkerhet i Gnesta kommun ska vara systematiskt och långsiktigt. Syftet är skapa en effektiv och säker informationsförsörjning. Hamnar informationen i fel händer, ändras eller förstörs kan det göra stor skada för både individen och kommunen.

Att säkerställa en god nivå av systematiskt informationssäkerhetsarbete möjliggör att:

- Lagkrav efterföljs
- kritisk verksamhet upprätthålls
- informationsläckage förhindras
- kontroll av kostnader uppnås
- förtroendet för kommunens tjänster och varumärke skyddas.
- kvaliteten och förtroendet för den kommunala verksamheten ökar.

Säker information genom klassning

Informationssäkerhetsklassning innebär att man värderar hur viktig informationen är för verksamheten och att informationstillgången tilldelas en skyddsnivå.

Varje verksamhet ansvarar för sin informationssäkerhet eftersom de har bäst kunskap om hur känslig och kritisk deras information är. Det innebär att verksamheten ställer krav på de aktörer som hanterar informationen. Det kan till exempel vara kommunens IT-avdelning, externa systemleverantörer eller leverantörer av molntjänster.

Verktyget KLASSA

I Gnesta kommun använder vi SKR:s verktyg KLASSA när vi gör en informationssäkerhetsklassning för att avgöra vilken skyddsnivå, information och verksamhetsprocesser ska ha.

Genom att klassa information kan vi identifiera känslig och kritisk information, och därefter vidta åtgärder så att informationen får rätt skydd. Informationen klassas utifrån aspekterna konfidentialitet, tillgänglighet och riktighet.

Varje enhet/förvaltningen ansvarar för att klassa sin information med hjälp av SKR:s verktyg KLASSA. Mer information om verktyget KLASSA hittar du på KLASSA - Start (skl.se)

Policyns roll i informationssäkerhetsarbetet

Policyn för informationssäkerhet redovisar kommunens övergripande systematiska arbete med informationssäkerhet. Policyn är utgångspunkt för:

- Riktlinje för informationssäkerhet
- Riktlinje för molntjänster
- Säkerhetsinstruktion för användare

Omfattning

Vad omfattas?

Informationssäkerhetspolicyn omfattar alla informationstillgångar som Gnesta kommun äger och hanterar. Detta gäller oavsett om informationen finns lokalt eller hos extern part i form av till exempel molntjänst eller hybridlösning. Exempel på informationstillgångar kan vara information som:

- Finns i datorer eller på servrar
- skickas med e-post, chatt eller liknande
- finns på mobila enheter (telefoner och surfplattor)
- finns lagrad på externt media (exempel USB-minne)
- visas på webbsidor eller via sociala medier
- överförs muntligt via ett samtal med telefon, direkt eller annan mötesplattform

- finns i skriftlig form på papper.

Vem omfattas?

Alla som hanterar informationstillgångar i Gnesta kommun omfattas av policyn. Den gäller samtliga anställda, förtroendevalda och uppdragstagare som arbetar med kommunens information. Informationssäkerhet är en integrerad del i Gnesta kommuns verksamheter och samtliga chefer ansvarar för att de själva och deras personal har kännedom om informationssäkerhetspolicyn och att dess innehåll följs.

Avgränsning

Internet och e-post

Förutsättningar och restriktioner för användandet av internet och e-post hanteras i Säkerhetsinstruktion för användare.

Molntjänster

Förutsättningar och restriktioner för användning av molntjänster hanteras i riktlinje för molntjänster.

Mål med informationssäkerhet

Gnesta kommun ska uppnå och upprätthålla en informationssäkerhet som:

- Innebär en robust, säker och tillförlitlig informationshantering.
- Möjliggör ett aktivt medverkande, både för anställda och kommuninvånare, i det digitala samhället.
- Bidrar till att verksamhetens uppsatta mål nås gällande exempelvis kvalitet, effektivitet och personlig integritet.
- Motsvarar medborgares och externa verksamheters behov och förväntningar.
- Uttrycks i aktuella styrdokument som policy och riktlinjer.
- Efterlever krav i lagar, förordningar, föreskrifter och avtal.
- Bidrar till ökad effektivitet genom rätt IT-stöd i förvaltningarna.
- Ger bättre förutsättningar för ledning, styrning, uppföljning, utvärdering och resursfördelning.

Gnesta kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot kommunens verksamheter vara vägledande och stödjande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Gnesta kommuns informationstillgångar. Samt att utforma och införa säkerhetsåtgärder som minskar dessa risker till en acceptabel nivå.

För att fastställa rätt nivå av skydd ska information klassificeras enligt kommunens klassningsmodell utifrån konfidentialitet, riktighet och tillgänglighet. Informationsägare är ansvarig för att detta arbete genomförs.

Utgångspunkter

Arbetet med informationssäkerhet i Gnesta kommun ska:

- Vara systematiskt och långsiktigt.
- Löpande ses över och förbättras eftersom Gnesta kommun och dess 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 kan inträffa.
- Bygga på Gnesta kommuns värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild.
- Bygga på en helhetssyn som utgår från information, men även innefatta processer, människor och teknik.

Metoder för att uppnå målen med informationssäkerhet

- Alla informationstillgångar ska vara identifierade och ha en informationsägare.
- Informationssäkerhetspolicyn ska användas vid kravställning inför upphandling, vid utveckling, användning och avveckling av informationstillgångar.
- Berörda medarbetare ska känna till informationssäkerhetspolicyn och utbildas för att öka säkerhetsmedvetandet.
- Kommunens informationssäkerhetsarbete ska ske i samverkan med myndigheter, företag och nätverk, som exempelvis SKR (Sveriges kommuner och regioner) och MSB (Myndigheten för samhällsskydd och beredskap).
- Nödvändiga åtgärder ska vidtas utifrån risk- och sårbarhetsanalyser samt inträffade incidenter för att säkerställa att informationen har rätt nivå av skydd.
- Skyddsåtgärder ska vara kostnadseffektiva. Kostnaden ska stå i proportion till värdet av informationen och de negativa konsekvenser som en otillräcklig säkerhet kan medföra.
- För att skydda informationstillgångar från avbrott och störningar behövs en kontinuitetsplanering.
- Informationssystem som är av vikt för Gnesta kommun ska genomgå en riskanalys. Riskanalysen ligger till grund för var driften av systemet ska vara och vilken skyddsnivå det ska ha.
- Rätt identitet och behörighet ska utgå utifrån ansvar och roll. Detta gäller vid nytt, ändrat eller avslutat behov.
- Informationssäkerhetspolicyn ska bidra till att personuppgifter och arkivering av information i Gnesta kommun behandlas korrekt.

Ansvar och roller

Alla medarbetare ska följa Gnesta kommuns informationssäkerhetspolicy och riktlinje för informationssäkerhet. Medarbetare ska vara uppmärksamma på brister och incidenter som rör informationssäkerheten och meddela sådant till systemägare och närmsta chef.

Alla som använder Gnesta kommuns informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för påföljder.

Nedan beskrivs informationssäkerhetsansvaret för olika funktioner och roller.

Kommunstyrelse

Kommunstyrelsen har det övergripande ansvaret för informationssäkerhet i Gnesta kommun.

Nämnder

Nämnderna har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom sina respektive verksamhetsområden. Varje nämnd ansvarar för att utse systemägare till de informationssystem som finns inom nämndens ansvarsområde.

Kommunchef

Kommunchef har kommunstyrelsens uppdrag att se till att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med policyn och tillhörande riktlinjer.

Verksamhetsansvariga

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Verksamhetsansvarig ska se till att medarbetarna har den kunskapen de behöver så att informationssäkerheten i verksamheten uppnås.

Informationsägare

Informationsägaren är den som äger och ansvarar för att:

- Informationen är riktig och tillförlitlig
- informationen hanteras enligt kommunens policy, riktlinjer och rutiner
- relevant lagstiftning följs
- informationsklassning genomförs.

Informationsägare utses av förvaltningschef eller motsvarande. I de fall en informationstillgång saknar informationsägare tillhör informationen det IT-stöd som informationen lagras i och ägs då av IT-stödets systemägare. Informationsägare kan även vara systemägare.

Informationsförvaltare

Informationsförvaltare är den som aktivt förvaltar informationen på informationsägarens uppdrag. Informationsförvaltare kan även vara systemförvaltare.

Systemägare

Systemägaren har det övergripande ansvaret för ett IT-system och är ansvarig för:

- All data i eller exporterat från informationstillgången
- att tillgången efterlever informationssäkerhetspolicyn med tillhörande riktlinjer
- att tillgångens informationssäkerhetsnivå sker enligt den beslutade modellen KLASSA.

Systemägaren ska utse systemförvaltare samt säkerställa att avtal för personuppgiftsbiträde finns i de fall detta är aktuellt.

Systemförvaltare

Systemförvaltaren ansvarar för hur systemet används. Systemförvaltaren ska se till att systemets funktionalitet, och planerade och beslutade aktiviteter, genomförs och upprätthålls.

IT-säkerhetsansvarig

IT-säkerhetsansvarig ansvarar för säkerheten i Gnesta kommuns IT-miljö oavsett var informationen lagras. IT-miljön ska vara tillförlitlig och motsvara interna och externa krav.

Informationssäkerhetsansvarig

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

Informationssäkerhetssamordnare

Informationssäkerhetssamordnare har det övergripande ansvaret för att leda, samordna och utveckla det strategiska informationssäkerhetsarbetet.

Dataskyddsombud

Dataskyddsombudets roll är att kontrollera att dataskyddsförordningen (GDPR) i Gnesta kommun följs. Dataskyddsombudet ska hjälpa till med den information, rådgivning och utbildning som behövs för att kommunens verksamheter ska kunna leva upp till krav som ställs av aktuellt lagrum.

Arkivarie

Arkivarien ansvarar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen.

Personuppgiftsansvariga

I Gnesta kommun är kommunstyrelsen och övriga nämnder i kommunen personuppgiftsansvariga. Det betyder att de både är ansvariga för hanteringen av personuppgifter och ska utse personuppgiftsombud som kontrollerar att personuppgifter hanteras på ett korrekt sätt i verksamheten.

Incidenthantering och rapportering

Alla som berörs av denna policy ska vara uppmärksamma på och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar. Rapportering sker till systemägare som i sin tur rapporterar till informationssäkerhetssamordnare.

Beslutsinstans och referensgrupper

- Informationssäkerhetspolicyn beslutas av kommunfullmäktige.
- Riktlinje för informationssäkerhet, riktlinje för molntjänster samt säkerhetsinstruktion för användare beslutas av IT-chef på delegation från kommunstyrelsen.

Revidering och uppföljning

I det systematiska informationssäkerhetsarbetet ska rutiner för uppföljning och kontroll ingå så att det regelbundet kan kontrolleras att skyddet upprätthålls. IT-chef är revisionsansvarig för informationssäkerhetspolicyn med tillhörande riktlinjer.