Gävle KOMMUN

Remissmissiv

Marie Ledesma
Marie.ledesma@gavle.se

Remissmissiv

Till	Samtliga nämnder och bolag
Ärende	Informationssäkerhetspolicy
Vårt dnr nr	19KS494
Handlingar	Remissmissiv Informationssäkerhetspolicy
Svarsdatum	2020-03-31

Remiss

Ny lagstiftning har tillkommit som ställer högre krav på kommunerna gällande informationssäkerhet.
På övergripande nivå finns krav på informationssäkerhet i Lag om informationssäkerhet i samhällsviktiga och digitala tjänster (2018:174) och i Dataskyddsförordningen.

I föreskrifterna till Lag om informationssäkerhet i samhällsviktiga och digitala tjänster (2018: 1175) ställs krav på ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017. I föreskrifterna står bland annat att en leverantör av samhällsviktiga tjänster ska upprätta en informationssäkerhetspolicy där ledningens målsättning och inriktning för organisationens informationssäkerhetsarbete framgår.

Nuvarande informationssäkerhetspolicy som beslutades av kommunfullmäktige 2017 är i behov av revidering varvid en ny informationssäkerhetspolicy har tagits fram.

Kommunstyrelsen efterfrågar särskilt synpunkter på de delar i policyn som avser mål med informationssäkerhetsarbetet samt roller och ansvar.

Era synpunkter ska skickas till kommunstyrelsen@gavle.se senast den 31 mars 2020. Förutom synpunkter på remissen skall också för besvarade nämnder och bolag ett protokollsutdrag bifogas.

Frågor under remisstiden besvaras av Marie Ledesma, informationssäkerhetssamordnare, 026-17 96 72.

Gävle
KOMMUN

Policy för informationssäkerhet i Gävle kommunkoncern

Policyns syfte

Denna policy är ett övergripande dokument som anger Gävle kommunkoncerns viljeinriktning och övergripande mål för informationssäkerhetsarbetet i kommunkoncernens verksamhetsområden. Samtliga kommunkoncernens verksamheter omfattas av denna policy.

Policyn gäller samtliga informationstillgångar som hanteras av Gävle kommunkoncerns verksamheter oavsett om den är förmedlad muntligt, pappersbundet eller digitalt.

Samtliga förtroendevalda, anställda, konsulter och andra som är i kontakt med kommunens informationstillgångar omfattas av denna policy och dess tillhörande styrdokument.

Informationssäkerhetspolicyn med kompletterande riktlinjer, rutiner och instruktioner ger koncernens verksamheter stöd i informationssäkerhetsarbetet och förutsättningar att uppnå sina verksamhetsmål. Respektive nämnd och styrelse ska anlaysera behovet av och eventuellt ta fram, egna rutiner/instruktioner för underliggande veksamheter till stöd för denna policy.

Hantering av personuppgifter ska följa dataksyddsförordningen.

Hantering av arkiv och allmänna handlingar ska följa arkivlagen, tryckfrihetsförordningen och offentlighets- och sekretesslagen.

Hantering av information som omfattas av säkerhetsskydd ska följa Säkerhetspolisens föreskrifter om säkerhetsskydd.

Verksamheter som omfattas av NIS-direktivet, dvs har identifierats som leverantörer av samhällsviktiga tjänster, ska följa Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster.

Om informationssäkerhet

Information finns och hanteras i alla kommunkoncernens verksamheter. Att information som kommunens nämnder och bolag hanterar (i interna och externa relationer) är tillgänglig för rätt person vid rätt tidpunkt samt att den är tillförlitlig är viktigt för att kommunens nämnder och bolag ska kunna utföra sina uppdrag och uppnå sina verksamhetsmål.

Bristande informationssäkerhet kan få konsekvenser i form av bristande skydd för den personliga integriteten eller störning i samhällsviktig verksamhet.

En god informationssäkerhet inom kommunens nämnder och bolag främjar verksamheternas funktionalitet, kvalitet och effektivitet, medborgares personliga integritet, kommunens förmåga att förebygga och hantera störningar och kriser, samt förtroenden hos medborgare, företag, myndigheter och organisationer för kommunkoncernens informationshantering och IT-system.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån fyra (säkerhets-) aspekter:

- **Konfidentialitet**: att informationstillgångar inte görs tillgängliga för obehörig.
- **Riktighet**: att informationstillgångar skyddas mot oönskad och obehörig förändring eller förstörelse.
- **Tillgänglighet**: att informationstillgångar är tillgängliga i förväntad utsträckning och inom önskad tid.
- **Spårbarhet**: att i efterhand kunna härleda specifika aktiviteter eller händelser rörande informationstillgångarna (vem, vad, när).

Information har olika grad av krav på sig gällande de fyra aspekterna. Arbetet med informationssäkerhet utgår framförallt från lagar, förordningar och föreskrifter men även nämnder och bolags egna krav och målsättningar är styrande.

Mål för informationssäkerhetsarbetet

Målet med informationssäkerhetsarbetet är att skydda kommunkoncernens information så att den alltid ska vara tillgänglig där den behövs, att det alltid ska gå att lita på att informationen inte är manipulerad eller förstörd, att informationen endast är tillgänglig för personer som är behöriga att få ta del av den och att det ska gå att följa hur och när informationen har hanterats och kommunicerats.

Gävle kommunkoncern ska uppnå och upprätthålla en informationssäkerhet som:

- innebär en säker och tillförlitlig informationshantering som är anpassad efter verksamhetens förutsättningar och behov,
- efterlever de krav som ställs på informationssäkerhet i lagar, förordningar, föreskrifter och avtal,
- utgår från etablerade standarder för informationssäkerhet (ISO/IEC 27001 och ISO/IEC 27002), ledningssystem för informationssäkerhet (LIS).
- skyddar informationstillgångar i nivå med dess värde och utifrån de negativa konsekvenser som otillräcklig informationssäkerhet kan medföra,
- styr åtkomst till information och informationsbehandlande resurser utifrån informationens känslighet och i den utsträckning som är lämplig för varje individs arbetsuppgifter.
- Löpande ses över och utvecklas (då omvärld och hot är under ständig förändring).

Strategier för att nå målen

För att uppnå målen med informationssäkerhet ska Gävle kommunkoncern sträva efter att:

- Alla informationstillgångar klassificeras, detta ska ligga till grund för införandet av rätt/adekvat skydd dvs säkerhetsåtgärder.
- Leva upp till de krav som de internationella informationssäkerhetsstandarderna SS-ISO/IEC 27001 och 27002 ställer på verksamheters informationssäkerhet.
- Upprätta, underhålla och testa planer mot avbrott i informationsflödet (kontinuitetsplanering).
- Alla incidenter för informationssäkerhet och personuppgifter rapporteras och följs upp.
- Alla som omfattas av denna policy har tillräcklig förståelse för och kunskap om informationssäkerhet och dataskydd för att kunna genomföra sina arbetsuppgifter på ett säkert sätt.
- Tillämpningen av policyn ska ske med stöd av riktlinjer för informationssäkerhet och underliggande rutiner och instruktioner.

Roller och ansvar

Informationssäkerhet är en integrerad del av det dagliga arbetet inom nämnder och bolags verksamheter. Alla och envar som hanterar information har därför ett ansvar att arbeta på ett säkert och ansvarsfullt sätt med informationstillgångar.

Kommunkoncernens informationssäkerhetssamordnare och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet, dataskydd eller andra relaterade frågor, fungerar som stöd till kommunkoncernens verksamheter att fullfölja informationssäkerhetsansvaret.

Kommunfullmäktige beslutar om informationssäkerhetspolicy för Gävle kommunkoncern. Nämnder och bolagsstyrelser ansvar för att informationssäkerheten upprätthålls inom respektive verksamhet.

Följande roller är centrala för det strategiska och operativa informationssäkerhetsarbetet i Gävle kommunkoncern.

- ***Kommunfullmäktige*** fastställer kommunkoncernens policy för informationssäkerhet.
- ***Kommunstyrelsen*** fastställer kommunkoncernes övergripande riktlinjer för informationssäkerhet.
- ***Nämnder och bolagsstyrelser*** ansvarar för:
  - informationssäkerheten inom sitt ansvarsområde.
  - att informationssäkerhetspolicyn med tillhörande riktlinjer efterlevs i verksamheten.
  - bedömer och beslutar om behov av särskilda rutiner/intstruktioner som stöd för denna policy.

- är personuppgiftsansvariga för hantering av personuppgifter i respektive verksamhet och formellt föremål för eventuell tillsyn.

- ***Samtliga chefer*** är ansvariga för att informationssäkerhetsarbetet bedrivs i linje med denna policy med tillhörande riktlinjer och rutiner/instruktioner inom sina respektive ansvarsområden.
- ***Dataskyddsombud***. Övervakar verksamheternas efterlevnad av dataskyddslagstiftningen samt ger råd och vägledning.
- ***Informationssäkerhetssamordnare*** ansvarar för övergripande samordning av informationssäkerhetsarbetet och övervakar att informationsskerhetspolicyn och tillhörande riktlinjer följs.
- ***Dataskyddssamordnare /mottagare informationssäkerhet*** Det ska finnas utesdda kontakpersoner av varje nämnd eller bolagsstyrelse, dessa ansvar för det löpande operativa arbetet med informationssäkerhet och dataskydd inom respektive verksamhet.
- ***Varje medarbetare och förtroendevald*** är ansvarig för att följa policy, riktlinjer och instruktioner för informationssäkerhet och dataskydd.
- ***Systemägare/objektägare*** har det övergripande ansvaret för respektive system och objekt och dess användning. System och objekt ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav.
- ***Informationsägare*** har det yttersta ansvaret för informationen. Informationsägaren avgör vilken information som får hanteras, hur den hanteras och av vem. Ställer krav på säkerheten för informationen. Informationsägarskapet följer verksamhetsansvaret.
- ***IT- och utvecklingschef*** har det övergripande ansvaret för att uppfylla de krav som nämnder och bolag ställer på den tekniska IT-infrastrukturen.

Den som använder kommunens informationstillgångar eller i övrigt agerar på ett sätt som strider mot denna policy eller övriga styrdokument avseende informationssäkerhet kan bli föremål för arbetsrättsliga påföljder. Vid misstanke om brott görs polisanmälan.

Uppföljning och rapportering

Informationssäkerhetspolicyn och tillhörande riktlinje för informationssäkerhet ska granskas och revideras minst vart tredje år, eller om betydande förändringar i organisation eller omvärld sker. Detta för att säkerställa policyns och riktlinjens fortsatta lämplighet, riktighet och verkan.

Informationssäkerhetssamordnaren ska årligen rapportera läge och status gällande informationssäkerhet till respektive nämnd eller bolagsstyrelse (”ledningens genomgång”). Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.