NÄSSJÖ KOMMUN

Författningssamling

Dokumenttyp Policy	Beslutsinstans Kommunfullmäktige	Beslutsdatum 2020-01-30	§ 16
Dokumentansvarig Avdelningschef digitalisering och innovation			
Gäller för Nässjö kommun och dess bolag		Senast reviderad	

Informationssäkerhetspolicy (höglandsgemensam)

Om denna informationssäkerhetspolicy

Informationssäkerhetspolicyn är ett dokument som redovisar kommunens övergripande mål och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.
Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Nässjö kommun, och kompletterar kommunens övriga styrdokument inom säkerhetsområdet. Hela kommunkoncernen omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna. Undantag för bolagen om det finns laglig grund.

Denna policy är fastställd av kommunfullmäktige och gäller från och med 2020-01-30.

Om informationssäkerhet

Information finns i alla kommunens verksamheter och handlar om allt vi gör och allt vi säger, exempelvis om vår personal, våra tjänster, vår ekonomi och det omgivande samhället med invånare, företag, föreningar med flera. Information är därför i sig en av kommunens viktigaste tillgångar.
För att nå hög kvalitet i vårt arbete måste information hanteras på rätt sätt. Det innebär att information finns tillgänglig när den behövs, att den är korrekt och att obehöriga inte får åtkomst till den. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser.
Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån fyra 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
- **Spårbarhet**: att händelser i informationsbehandlingen ska kunna spåras

Kraven på hantering av information styrs av lagar, förordningar och kan kompletteras med Nässjö kommuns egna målsättningar. Dessutom har självklart den enskilde, företag 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. En informationstillgång innebär allt som innehåller information och allt som bär på information.

Mål med informationssäkerhet

Målet för Nässjö kommuns informationssäkerhetsarbete är att hantera och skydda informationen i verksamheterna på sådant sätt att rättsliga och verksamhetsmässiga krav, samt invånarintressen kan tillgodoses. Detta skapar en robust, säker och tillförlitlig informationshantering i hela organisationen.
Skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav och ska därigenom möjliggöra för kommunens verksamheter att uppnå sina mål. En god informationssäkerhet inom kommunen främjar verksamheternas funktionalitet, kvalitet och effektivitet. Dessutom främjas invånarens rättigheter och personliga integritet, kommunens förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för kommunens informationshantering och IT-system.

Principer och arbetssätt

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

Arbetet med informationssäkerhet inom Nässjö kommun ska:

- vara systematiskt och bygga på etablerade standards (ISO 27000) med målet att skapa ett ledningssystem för informationssäkerhet (LIS från Myndigheten för samhällsskydd och beredskap MSB). Systematiken innebär kontinuerliga uppföljningar med reviderade handlingsplaner enligt metodiken planera, genomföra, följa upp och åtgärda. För att säkerställa kvalitet och objektivitet sker intern och extern granskning enligt fastställd regelbundenhet.
- utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder (planeras och dokumenteras i handlingsplan) för att se till att vår information har rätt skydd. Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.
- ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationstillgångar och uppföljning av ställda krav ska ske kontinuerligt.
- ska utgå från kontinuitetsplanering och ha beredskap för avbrott och störningar. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter. Detta ska övas regelbundet genom olika simulerade informationssäkerhetsincidenter.
- utgå ifrån att alla anställda och förtroendevalda vet vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas. Det är viktigt att alla anställda och förtroendevalda har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.
- säkerställa rätt identitet och behörighet utifrån roll, för alla som får tillgång till information. Det gäller vid nytt, ändrat eller avslutat behov.
- utgå ifrån att alla informationstillgångar är identifierade och dokumenterade. Hantering av personuppgifter ska följa särskilda riktlinjer. All information ska sparas, alternativt gallras, enligt gällande lagstiftning och finnas dokumenterat.

Verksamhetsdriven informationssäkerhet genom informationsklassning

Verksamheterna har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras information är, och därmed kunskap om informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheterna, utifrån informationens skyddsvärde, ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts- och 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. Informationen ska systematiskt definieras (enligt Samrådsgruppens ”Klassa”) och värderas (enligt SKLs ”KLASSA”).
Nässjö 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, tillgänglighet och spårbarhet.

Roller och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Det gäller från koncernledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssamordnare eller motsvarig och övriga som arbetar specifikt med informationssäkerhet, IT-säkerhet eller andra relaterade frågor, fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret. Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvar och tillhörande uppgifter för respektive roller beskrivs utförligare i riktlinjer inom informationssäkerhetsområdet.

Kommunfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för kommunen. Vid behov ska fullmäktige initiera revidering av policyn men minst en gång per mandatperiod.

Kommunstyrelsen ansvarar för samordningen av informationssäkerhetsarbetet i kommunen och ska därför årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet.

Varje nämnd och bolagsstyrelse ansvarar för informationssäkerheten inom sitt verksamhetsområde och ska därför, inom ramen för sitt lokala ledningssystem och i enlighet med policy och riktlinjer, anta verksamhetsnära styrdokument för informationssäkerhet. Varje nämnd och bolagsstyrelse ska årligen planlägga och löpande följa upp informationssäkerheten, och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla en robust, säker och tillförlitlig informationshantering.

Kommundirektör och Vd har kommunstyrelsens eller bolagsstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer.

Kommundirektören ansvarar för att övergripande riktlinjer utarbetas och hålls aktuella i enlighet med policy. Vd ansvarar för att lokala riktlinjer utarbetas och hålls aktuella.

Verksamhetsansvariga, oavsett nivå, ansvarar för informationssäkerheten inom sin verksamhet. Varje verksamhetsansvarig ansvarar för att egna medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en nödvändig informationssäkerhet i verksamheten kan uppnås.

Medarbetare och förtroendevalda har ett ansvar att följa kommunens informationssäkerhetspolicy och riktlinjer för informationssäkerhet. Man har som medarbetare och förtroendevald också ansvar att vara uppmärksam på brister och fel gällande informationshantering, utrustning och informationsinnehåll, och rapportera sådana enligt fastställda rutiner.

Systemägare är informationsansvarig för all data i, eller exporterat från, informationstillgången. I ansvaret ingår även att tillgången efterlever informationssäkerhetspolicy och riktlinjer för informationssäkerhet. En viktig del i ansvaret är att besluta om tillgångens informationssäkerhetsnivå genom att klassning sker enligt beslutad modell. Systemägaren ska utse systemansvarig, samt säkerställa att avtal för personuppgiftsbiträde finns. I Nässjö kommun är förvaltningschef samt kommunledningskontorets avdelningschefer systemägare.

Systemansvarig är den eller de personer i berörda verksamheter eller hos annan part som har ansvaret för den dagliga användningen av det digitala verksamhetsstödet.

Höglandets IT (HIT) ansvarar för att säkerheten i kommunens IT-miljö är tillförlitlig och motsvarar interna (verksamhetens) och externa (legala) krav. IT-miljön ska även uppfylla de krav som denna informationssäkerhetspolicy och underliggande riktlinjer för informationssäkerhet ställer. Höglandsförbundets antagna IT-säkerhetspolicy styr detta arbete.

Driftansvarig för informationstillgång innehar den tekniska kompetensen och ansvarar tillsammans med systemansvarig för att den dagliga driften upprätthålls enligt avtal.

Höglandets nätverk för informationssäkerhet ska driva det övergripande och strategiska arbetet med att utveckla och samordna informationssäkerhetsarbetet för höglandskommunerna. Informationssäkerhetsspecialist ska arbeta i samråd med kommunernas kontaktpersoner vad gäller informationssäkerhet.

Kommunarkivet har tillsynsansvar för att informationen hanteras enligt bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen, samt kommunens interna styrdokument rörande informationens långsiktiga hantering och bevarande.

Personuppgiftsansvariga är kommunstyrelsen, övriga nämnder och bolagsstyrelser i kommunen. Dessa är ansvariga för behandling av personuppgifter och ska utse dataskyddsombud som kontrollerar att personuppgifter behandlas på ett korrekt sätt i verksamheten.