KOMMUNKANSLIET

Datum: 2024-11-05

Policy för informationssäkerhet

Handläggare: Sara Dahlin och Rebecca Tellander

Innehåll

Inledning

Denna policy utgör kommunens viljeinriktning för att hantera kommunens information på ett systematiskt och informationssäkert sätt. Avesta kommuns informationssäkerhetpolicy omfattar all information som kommunens verksamheter äger och hanterar. Information är en av kommunens viktigaste tillgångar och är en förutsättning för att kommunens verksamheter ska kunna bedrivas, effektiviseras och nå sina mål. Informationssäkerhetsarbetet ska vara ett effektivt stöd i kärnverksamheten. Det systematiska arbetet med informationssäkerhet ska utgå från standarden för informationssäkerhet enligt ISO 27000-serien och integreras i kommunens styrmodell. Lagar och förordningar utgör en grund för detta arbete, överenskomna avtal ska följas och medborgarnas krav och förväntningar införlivas.

Detta dokument är en del av ledningssystemet för informationssäkerhet (LIS). I ledningssystemet för informationssäkerhet ingår förutom denna policy även riktlinjer och rutiner som täcker ett flertal områden. LIS för Avesta kommun omfattar alla kommunens nämnder och helägda kommunala bolag. Detta styrdokument och andra relevanta styrdokument kring informationssäkerhet och dataskydd gäller även för externa aktörer när dessa använder sig av Avesta kommuns och/eller dess bolags informationstillgångar.

Definition av information

Information är upplysningar om faktiska och tänkta förhållanden och kan innehålla uppgifter om personer. Information kan uttryckas i och representeras av mänskliga tankar och kunskaper, ord som skrivs på papper, tal som förmedlas muntligt eller via telefon eller data i form av tecken och signaler i olika digitala och analoga media. Information finns i kommunens alla verksamheter och är en värdefull, viktig och kritisk tillgång.

Informationssäkerhet

Informationssäkerhet handlar om säkerhet för information. Det innebär att se till att informationstillgångar finns tillgängliga när de behövs, att de är korrekta och att obehöriga inte får åtkomst till dem. En väl utvecklad och integrerad informationssäkerhet bidrar till att etablera en effektiv och ändamålsenlig informationshantering, vilket skapar förtroende både inom och utanför organisationen och direkt bidrar till att:

- undvika incidenter,
- säker verksamhetsutveckling,
- bevara förtroende hos medborgarna, samt
- införa en metodik och ett arbetssätt för att efterleva lagstiftning och löpande uppföljning.

Informationssäkerhet är verksamhetsorienterat, eftersom det handlar om säkerhet för information som har tillskrivits ett värde och en betydelse i en verksamhetskontext. Informationens relevans och värde är avgörande vid bedömning av vilken grad av skydd som är rimlig i en viss situation. Det är informationens värde som styr vilken säkerhet som krävs, i form av till exempel fysiskt skydd som lås, passersystem och brandskydd eller vilken IT-säkerhet som krävs. Informationssäkerhet handlar om bevarande av konfidentialitet, riktighet och tillgänglighet.

- Konfidentialitet: att information enbart är tillgänglig för behöriga.
- Riktighet: att information är korrekt, tillförlitlig och fullständig.

- Tillgänglighet: att information är åtkomlig i rätt tid och användbar av behörig.

Informationssäkerhet begränsas inte till säkerhet i IT-resurser utan omfattar information i alla dess former och oavsett hur informationen hanteras. Informationssäkerhetsarbetet ska bedrivas så det stödjer kommunernas arbete samtidigt som det skyddar kommunens, medarbetarnas och invånarnas information. Ansvaret för informationssäkerheten ska följa verksamhetsansvaret. Alla chefer, medarbetare och förtroendevalda ansvarar för att denna policy och tillhörande riktlinje följs då de hanterar kommunens informationstillgångar. Informationssäkerhetsarbetet ska säkerställa att informationstillgångarna skyddas utifrån informationstillgångens skyddsvärde oavsett om den hanteras analogt eller digitalt.

Lagstiftning

På övergripande nivå finns krav på informationssäkerhet i tryckfrihetsförordningen, offentlighets- och sekretesslagen, dataskyddsförordningen (GDPR) och lag om informationssäkerhet i samhällsviktiga och digitala tjänster (NIS2-direktivet) samt säkerhetsskyddslagen. Därutöver finns verksamhetsspecifika krav på informationssäkerhet i bland annat i skollagen, socialtjänstlagen, hälso- och sjukvårdslagen och patientdatalagen.

Dataskyddsförordningen ställer krav på hantering av personuppgifter. Informationstillgångar som lyder under NIS2-direktivet är de som berör leverantörer av samhällsviktiga tjänster. Till kommunens samhällsviktiga tjänster räknas bland annat energi, hälso- och sjukvård, avfallshantering samt dricks- och avloppsvatten. Säkerhetsskyddslagen avser Sveriges säkerhet och berör bara säkerhetskänsliga verksamheter. Skollagen, socialtjänstlagen och hälso-och sjukvårdslagen ställer krav på tystnadsplikt och sekretess.

Globala målen i Agenda 2030

Agenda 2030 är en integrerad del i Avesta kommuns styrmodell. Ett av hållbarhetsmålen, mål 16, handlar om det fredliga och inkluderande samhället. Det handlar bland annat om att alla människor är lika inför lagen och ska ha lika tillgång till rättvisa samt ska ha möjlighet att utöva inflytande och ansvarsutkrävande över beslutsfattare. God samhällsstyrning och rättsstatens principer är grundläggande mål och medel för en god demokratisk utveckling. Mål 16 har ett delmål i 16.10 att säkerställa allmän tillgång till information och skydda grundläggande friheter, i enlighet med nationell lagstiftning och internationella avtal. Kommunens arbete med informationssäkerhet och dataskydd är viktiga delar för att uppnå hållbarhetsmålet.

Tillsynsmyndigheter

Informationssäkerhetsarbetet stöds och följs upp från flera myndigheter och organisationer, bland annat:

- Länsstyrelsen,
- Myndigheten för samhällsskydd och beredskap (MSB),
- Sveriges kommuner och regioner (SKR),
- Integritetsskyddsmyndigheten (IMY),

- Statens energimyndighet,
- Livsmedelsverket,
- Inspektionen för vård och omsorg (IVO),
- Säkerhetspolisen.

Syfte med informationssäkerhetsarbete

Syftet med en god informationssäkerhet är att tjänster av god kvalitet ska kunna levereras till de som kommunen är till för. Ledningssystemet ska också stödja kommunen i att efterleva lagar, förordningar, föreskrifter och avtal.

Avesta kommun ska uppnå och upprätthålla informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering,
- i möjligaste mån motsvarar medborgares och externa verksamheters behov och förväntningar,
- möjliggör och underlättar utveckling och att den sker med tillräcklig säkerhet,
- möjliggör att samtliga kritiska informationstillgångar informationsklassas.

Principer för informationssäkerhetsarbetet

Systematiskt informationssäkerhetsarbete

Avesta kommuns ledningssystem för informationssäkerhet ska uppfylla de grundläggande kraven på systematiskt informationssäkerhetsarbete enligt ISO 27000-serien och kommunen ska tillämpa ett arbetssätt som stödjer ständiga förbättringar.

Kommunen ska uppfylla nuvarande och tillkommande lagkrav som berör kommunen och som kräver ett systematiskt informationssäkerhetsarbete.

Organisation

Avesta kommun ska upprätta en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete. En riktlinje ska finnas som beskriver organisation och roller för informationssäkerhetsarbetet.

Hantering av informationstillgångar

Samtliga chefer, medarbetare och förtroendevalda ska erbjudas relevant utbildning inom informationssäkerhet. Informationssäkerhetsansvarig ansvarar för att det finns lämpligt och målgruppsanpassat utbildningsmaterial. Chefer ansvarar för att medarbetare har rätt behörighet och förutsättningar att i sitt arbete hantera kommunens informationstillgångar.

Avesta kommun ska fastställa informationssäkerhetsrelaterade krav på bakgrundskontroll för befattningar. Bakgrundskontroller ska vara anpassade till olika befattningar beroende på vilken information medarbetaren ges tillgång till. Kommunen ska sträva efter att skapa en god säkerhetskultur i hela

organisationen. Detta uppnås främst genom styrande dokument och att medarbetare och förtroendevalda utbildas i informationssäkerhet. Vidare ska avvikelser och risker hanteras som underlag till ständiga förbättringar.

Det ska finnas ett fungerande samspel mellan olika kompetenser inom säkerhet, informationssäkerhet, IT, juridik och ledning. Riktlinjer ska finnas för informationssäkerhet för medarbetare och förtroendevalda.

Fysisk och teknisk säkerhet

Avesta kommun ska fastställa kraven på den fysiska och tekniska säkerheten i de system som hanteras av kommunens IT-enhet eller av andra leverantörer och säkerställa att kraven uppfylls. En riktlinje ska finnas som beskriver fysisk och teknisk säkerhet.

Leverantörsrelationer

Avesta kommun ska fastställa de informationssäkerhetsrelaterade krav som ska användas vid upphandlingar och i avtal med leverantörer framför allt av IT-system och IT-drift. Kommunen ska säkerställa skyddet för de informationstillgångar som leverantörer har åtkomst till genom att informationssäkerhetskrav ingår i leverantörsavtalen. Kommunen ska följa upp att leverantörerna lever upp till kraven på informationssäkerhet. Riktlinjer ska finnas som beskriver hur detta ska genomföras.

Hantering av informationssäkerhetsincidenter

Avesta kommun ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter. Incidentrapportering krävs för att uppfylla vissa lagkrav. Rutiner för avvikelsehantering och incidentrapportering ska finnas.

Efterlevnad

Efterlevnaden av informationssäkerhetsarbetet ska följas upp till exempel via internkontroll, revisioner och i ledningens förbättringsarbete.