Vindelns Kommun

2021-07-07 K-2021- 284

Riktlinjer för informationssäkerhet

Antagen av kommunstyrelsen den 14 september 2021, § 107

Vindelns Kommun

Innehållsförteckning

1. Inledning

Säkerhetsskyddet regleras i säkerhetsskyddslagen och säkerhetsskyddsförordningen. Nuvarande lagstiftning trädde i kraft den 1 april 2019. Den gäller för alla som bedriver säkerhetskänslig verksamhet, såväl allmänna som enskilda verksamhetsutövare. Säkerhetsskydd delas enligt lagen upp i de tre områdena:

- informationssäkerhet,
- fysisk säkerhet och
- personalsäkerhet.

Dessa riktlinjer hanterar informationssäkerheten. Intern säkerhet (fysisk säkerhet och personalsäkerhet) hanteras i Riktlinjer för intern säkerhet Dnr K-2021- 296.

Alla verksamheter är beroende av att kunna inhämta, lagra, bearbeta och kommunicera information i olika former. Den tekniska utvecklingen har på senare år gjort informationssystem till viktiga verktyg i hanteringen, men även pappersdokument används fortfarande. Säkerhetsskyddsåtgärden informationssäkerhet syftar till att skydda information oavsett form och förekomst, elektronisk såväl som fysisk. Informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Informationssäkerhet ska även förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

”*Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.* ” (2 kap. 2 § säkerhetsskyddslagen)

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för exempelvis digitalisering och för att verksamheterna ska nå sina mål. Att information som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation är korrekt, utgör en grund för tillit och förtroende. Det är även viktigt att information är tillgänglig när det behövs och att känslig information skyddas för att vi skall kunna fullgöra vårt uppdrag i samhället. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheter och alla de informationstillgångar som vi äger eller hanterar.

1.1 Syfte

Denna riktlinje utgör kommunens viljeinriktning för att hantera kommunens information på ett systematiskt och informationssäkert sätt.

1.2 Målgrupp

Riktlinjen omfattar förtroendevalda, chefer, medarbetare och uppdragstagare inom Vindelns kommun och dess bolag.

1.3 Definition av information/informationstillgång

Kommunen är beroende av information för att kunna utföra sitt uppdrag. Information kan exempelvis vara text, ljud, bild, film och tal. Personuppgifter är en vanligt förekommande och skyddsvärd information. Information finns överallt och kan förekomma i många olika former – tryckt eller skrivet på papper, lagrad elektroniskt i IT-utrustning och på lagringsmedia, överföras med post och elektronisk utrustning, yttras i en konversation och vara en del av en persons kunskap.

1.4 Definition av informationssäkerhet

Informationssäkerhet handlar om att skydda kommunens information så att:

- informationen alltid finns när vi behöver den (tillgänglighet)
- informationen är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer kan ta del av informationen (konfidentialitet)

1.5 Ansvar

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens informationssäkerhetssamordnare tillika Säkerhetschef och övriga som arbetar med IT-säkerhet eller andra relaterade frågor fungerar som stöd till kommunens verksamheter att uppfylla informationssäkerhets-ansvaret. Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.

Kommunstyrelsen uttrycker sin viljeinriktning rörande kommunens arbete med informationssäkerhet i denna riktlinje. Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet.

Nämnder/styrelser 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 får hanteras och av vem den får hanteras.

Anställda, förtroendevalda och uppdragstagare ansvarar för att följa de informationssäkerhetsriktlinjer och instruktioner som finns samt att agera säkerhetsmedvetet.

2. Strategiska mål med informationssäkerhet

Vindelns kommun bedriver ett långsiktigt och systematiskt informationssäkerhetsarbete,

vilket bygger på etablerade standarden för informationssäkerhet (ISO 27000-serien).

2.1 Målsättning

- Kommunens information skyddas på en lämplig administrativ och teknisk nivå, utifrån genomförda informationssäkerhetsklassificeringar och riskanalyser
- Det finns en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete.
- Chefer, medarbetare och förtroendevalda ska genomgå relevant utbildning inom informationssäkerhet

2.2 Principer för informationssäkerhet

Informationssäkerhetsarbetet i kommunen ska bedrivas systematiskt, formaliserat och riskorienterat. Informationssäkerhet är en grundförutsättning för att uppnå kvalitet och effektivitet i verksamheten, samt en förutsättning vid upphandling, digitalisering och mobilitet. Informationssäkerhetsarbetet ska skydda kommunens, medarbetarnas och medborgarnas information.

3. Uppföljning och efterlevnad/rapportering

3.1 Uppföljning

Kommunen ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter.

3.2 Efterlevnad

Informationssäkerhetssamordnaren tillika Säkerhetschefen ska en gång per år rapportera läge och status gällande informationssäkerhet till kommunstyrelsen och till kommunens ledningsgrupp. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar. Efterlevnaden av informationssäkerhetsarbetet ska följas upp via internkontroll. Förbättringsarbetet ska genomföras genom kontinuerlig återrapportering till ledningsgruppen.

4. Organisation och roller

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller.

Kommundirektör har det övergripande ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten.

Informationsägare är den som bestämmer ändamålen för behandlingen och hanteringen av informationen. Informationsägaren äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

Systemägare/objektägare har ansvaret för den verksamhet som aktuellt informationssystem/-objekt stödjer.

Systemförvaltare/objektförvaltare tar det funktionella (dagliga) helhetsansvaret för ett system/objekt. Förvaltaren fungerar i hög grad som system-/objektägarens utförare och ser till att systemets/objektets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Säkerhetschef ansvarar för informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Beredskapssamordnare genomför säkerhetsanalyser på uppdrag av säkerhetschefen.

Dataskyddsombudets roll är att regelbundet utbilda, rådgöra och granska nämndernas informationssäkerhet, med särskilt fokus på att granska efterlevnaden av dataskyddsförordningen.

Informationssäkerhetsamordnare tillika Säkerhetschefen har det övergripande ansvaret för att leda, utveckla och samordna arbetet med informationssäkerhet i kommunen. Stödfunktion för ledning och verksamheter.

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen har ett särskilt ansvar för den tekniska IT-säkerheten.

Kontaktombud, inom varje nämnd ska det finnas ett utsett kontaktombud vilket har ansvaret att dokumentera sin nämnds behandlingar av personuppgifter i en registerförteckning.

5. Revidering

Informationssäkerhetsriktlinjen skall revideras vid behov och ansvarig för detta är kommunens Säkerhetschef.