PM

Beskrivning av hur det kommunövergripande informationssäkerhetsarbetet ska bedrivas och organiseras

Inledning

Utifrån kommundirektörens beslut, den 31 maj 2023, presenterades, i oktober 2023, ett förslag på hur det kommunövergripande informationssäkerhetsarbetet ska bedrivas och organiseras.

Den övergripande inriktningen i förslaget har varit att den kommunövergripande styrningen och ledningen över informationssäkerheten ska tydliggöra fokus på regulatorisk compliance.

Förslaget innebär att merparten av det praktiska arbetet kommer att integreras i pm3, såsom kommunens styr- och samverkansmodell. Synergi- och samordningseffekter ska uppnås mellan informationssäkerhet, it-säkerhet och dataskydd.

I enlighet med vad som framgår nedan ska verksamhetens ansvar för genomförande och efterlevnad utökas och förstärkas. För att underlätta detta, samt för att stötta verksamheten rörande informationssäkerhet samt tydliggöra dess roll i pm3, ska respektive förvaltningschef utse minst en informationssäkerhetssamordnare.

Syfte

Informationssäkerhetsarbetet påverkas alltmer av såväl befintlig som kommande lagstiftning. Kommunen behöver leva upp till de ökade krav som ställs utifrån denna lagstiftning. Det ställer höga krav på kommunens förmåga att prioritera och införa väsentliga insatser, på såväl kommunövergripande som på förvaltnings-/objektsnivå. Det finns därför ett behov av en ständigt aktuell kommunövergripande bild av informationssäkerhetsrisker och sårbarheter. Denna bild ska användas vid olika prioriteringar inom informationssäkerhetsområdet samt för att ta fram riskbaserad planering av informationssäkerhetsåtgärder utifrån respektive verksamhets behov.

Ett ytterligare syfte är att, där så är möjligt, uppnå sammanhängande processer för dataskydd, informationssäkerhet och it-säkerhet, eftersom det har framkommit behov av att effektivisera arbetet på dessa områden.

Slutligen syftar arbetet till att belysa att det är allas ansvar att verka för en god informationssäkerhet. Det är därför viktigt att varje medarbetare ska ha en reell möjlighet att göra rätt val utan att vara specialist på området. I de fall brister inom informationssäkerheten upptäcks har alla ett ansvar att påtala sådana brister så att de kan åtgärdas.

Styrning av informationssäkerhet

Informationssäkerhet består av två delar - administrativ säkerhet och teknisk säkerhet. Med administrativ säkerhet avses säkerhetsåtgärder relaterade till hur kommunen styr informationssäkerhetsarbetet inom verksamheterna - formellt såväl som informellt. Med formell säkerhet avses i detta sammanhang, kommunövergripande rutiner för styrning och ledning av informationssäkerhet. Med informell säkerhet avses människors uppfattningar, värderingar och attityder som påverkar deras agerande i informationssäkerhetsfrågor, dvs. säkerhetsmedvetenhet och ökad säkerhetskultur. Juridikenheten ansvarar för den formella säkerheten och Utvecklings- och digitaliseringsenheten ansvarar för den informella säkerheten samt för teknisk säkerhet, vilken inte beskrivs närmare här, utan i andra styrdokument.

Juridikenhetens ansvar

Juridikenheten ansvarar för framtagande av kommunövergripande styrande dokument samt för att förvalta och följa upp redan befintliga styrdokument, inklusive att revidera kommunens ledningssystem för informationssäkerhet.

I juridikenhetens ansvar ingår att säkerställa att de kommunövergripande styrdokumenten tillser att kommunen efterlever relevanta lagar och regler samt att följa upp resultatet och föredra detta inför kommunledningen.

Juridikenheten ansvarar även för att leda, prioritera och samordna den kommunövergripande uppföljningen av informationssäkerhetsarbetet.

Juridikenhetens ansvar inom informationssäkerhetsområdet ska ske med ett särskilt fokus på regelefterlevnad inom området.

Juridikenheten ansvarar vidare för att ställa krav på och följa upp förvaltningarnas efterlevnad av styrande dokument samt vara ett stöd för förvaltningarna vid framtagande av förvaltningsspecifika rutindokument och vid implementeringen av dessa. Häri ingår att bistå med rådgivning och att delta i eller självständigt hålla utbildningar inom området.

Juridikenheten ansvarar härutöver för att vidmakthålla en nära samverkan med utvecklings- och digitaliseringsenheten, i syfte att hålla samman informations- och it-säkerhetsarbetet inom kommunen, för att nå en effektiv styrning inom området.

Informationssäkerhetsansvarig kommunjurist

Informationssäkerhetsansvarig kommunjurist (nedan informationssäkerhetsansvarig), som utses av chefsjuristen, är sammanhållande för det strategiska arbetet med att utveckla, förvalta och följa upp kommunens ledningssystem för informationssäkerhet och rapporterar till kommundirektören.

Informationssäkerhetsansvarig ska bistå nämnder och förvaltningar med rådgivning samt följa upp det kommunövergripande informationssäkerhetsarbetet. Uppföljningen ska ge stöd åt arbetet med att utveckla och förbättra ledningssystemet för informationssäkerhet.

Som stöd till den kommunövergripande informationssäkerhetsansvarige inrättas dels ett forum för informations- och it-säkerhet, dels en strategisk arbetsgrupp för informationssäkerhet. Informationssäkerhetsansvarig är också sammankallande för forumet för informations- och it-säkerhet. Informationssäkerhetsansvarig leder den strategiska arbetsgruppen för informationssäkerhet samt nätverket för informationssäkerhetssamordnarna (förkortas ISAM).

Informationssäkerhetsansvarig ska även ha en nära samverkan med dataskyddsombuden samt vid behov med nätverket för dataskyddssamordnare.

Informationssäkerhetsansvarig ska tillsammans med It-säkerhetsansvarig ansvara för att upprätthålla en ständigt aktuell kommunövergripande bild över informationssäkerhetsrisker och sårbarheter, vilken ska presenteras för såväl forumet för informations- och it-säkerhet som för kommundirektören.

Utvecklings- och digitaliseringsenhetens ansvar

Utvecklings- och digitaliseringsenheten ansvarar för att leda, prioritera och samordna det kommunövergripande it-säkerhetsarbetet, med fokus på efterlevnad av kommunens ledningssystem för informationssäkerhet. Med detta avses delar av den tekniska säkerheten samt de delar av informationssäkerheten som inte åligger juridikenheten eller verksamheterna, det vill säga den informella säkerheten. Med informell säkerhet avses i detta sammanhang såväl säkerhetsmedvetenhet som ökad säkerhetskultur inom informationssäkerhetsområdet. Till stor del ska detta utföras inom ramen för pm3. Utvecklings- och digitaliseringsenhetens ansvar innebär bl.a. att följa upp och utvärdera att beslutade skyddsåtgärder följer uppsatt regelverk samt upprätthålla en ständigt aktuell kommunövergripande bild över informationssäkerhetsrisker och sårbarheter.

It-säkerhetsansvarig

It-säkerhetsansvarig och informationssäkerhetsansvarige är varandras närmaste samverksansparter. Nedan redovisas därför det ansvar som it-säkerhetsansvarig har inom informationssäkerhetsområdet. Därutöver har it-säkerhetsansvarig ett omfattande ansvar inom it-säkerhet, vilket inte redovisas närmare här.

It-säkerhetsansvarig, som utses av Utvecklings- och digitaliseringschef, ska utveckla och upprätthålla kommunövergripande metoder och rutiner för informationssäkerhet utifrån fastställd styrdokumentation.

It-säkerhetsansvarig ska ansvara för att följa upp och utvärdera att beslutade skyddsåtgärder följer uppsatta regelverk.

It-säkerhetsansvarig ska ansvara för och ställa krav på en god säkerhetsmedvetenhet och informationssäkerhetskultur på såväl individnivå, förvaltningsnivå samt inom ramen för pm3.

It-säkerhetsansvarig ska även utforma gemensamma rutiner bl.a. för hantering av informationssäkerhetsincidenter samt utforma informationssäkerhetsmål som stödjer kraven på incidenthantering.

It-säkerhetsansvarig ska tillsammans med Informationssäkerhetsansvarig ansvara för att upprätthålla en ständigt aktuell kommunövergripande bild över informationssäkerhetsrisker

och sårbarheter, vilken ska presenteras för såväl forumet för informations- och it-säkerhet som för kommundirektören.

Forum för informations- och it-säkerhet

Ett forum för informations- och it-säkerhet ska inrättas i syfte att vara en samlad rapporteringsväg till kommundirektören i kommunövergripande informations- och it-säkerhetsfrågor. Forumet ska därför hållas uppdaterat om den kommunövergripande lägesbilden som presenteras av informations- och it-säkerhetsansvariga. Forumet ska, bl.a. utifrån de risker och sårbarheter som framkommer i lägesbilden, bedöma behov av åtgärder samt prioritera dessa i förhållande till varandra. Detta ska i huvudsak baseras på riskernas väsentlighet på kommunövergripande nivå. Forumet ska utifrån detta ge rekommendationer till kommundirektör eller kommunikations- och utvecklingsdirektör, om lämpliga åtgärder.

Informations- och it-säkerhetsansvariga avgör därutöver vilka ärenden som behöver lyftas från strategiska arbetsgrupperna till forumet. Som huvudregel gäller att endast de ärenden som är av principiell betydelse eller annars av större vikt för kommunens informationssäkerhet ska lyftas till forumet.

Forumet ska följa upp efterlevnaden av lagar och regler samt införda säkerhetsåtgärder. Forumet för informations- och it-säkerhetsfrågor består alltid av informationssäkerhetsansvarig (sammankallande) och it-säkerhetsansvarig och är primärt ett beredningsorgan men med visst beslutsmandat i de fall det särskilt framgår. Vid behov adjungeras, beroende på ärende, chefsjurist, chef för utvecklings- och digitaliseringsenheten, säkerhetsskyddschef, säkerhetschef eller it-chef. Därutöver kallas vid behov ansvarig direktör för kommunens it-säkerhet. Samtliga förslag som ska rapporteras från forumet till kommundirektören ska beredas, föredras och godkännas av ansvarig/ansvariga chef/chefer enligt ovan.

Förvaltningens ansvar

Informationssäkerheten är verksamhetsdriven. Det är förvaltningen som ska ha kunskap om

- vilka lagrum och övriga regulatoriska krav som verksamheten omfattas av,
- vilka medborgarnas/brukarnas/verksamhetens behov är,
- vilken information och data som lagras och vad som behövs för verksamheten (informationshanteringsplan),
- vilken säkerhetsnivå som ska råda för informationen och hur denna ska klassas,
- vilka behörigheter och åtkomster som viss personal behöver i sitt uppdrag,
- vilka krav på tillgänglighet som ska gälla,
- vilka risker, hotbilder och konsekvenser som finns inom verksamheten.

Verksamheten ansvarar för att kanalisera sina behov genom respektive pm3-objekt, där upprätthållande av it-säkerheten också tas omhand.

Förvaltningschefen ska styra och följa upp informationssäkerhetsarbetet. Till stöd för detta ska verksamheten ha minst en informationssäkerhetssamordnare vars ansvar beskrivs nedan. I förvaltningens informationssäkerhetsarbete ska riskernas väsentlighet vara styrande för att medvetna prioriteringar ska kunna göras av förvaltningen.

Informationssäkerhetssamordnarens ansvar

Informationssäkerhetssamordnaren, som utses av förvaltningschef, ska arbeta utifrån förvaltningschefens styrning avseende vilka verksamhetsrisker och åtgärder som ska prioriteras. Informationssäkerhetssamordnaren förutsätts därför ha god kännedom om såväl verksamheten i stort som dess informationshanteringsplan och dataskyddsarbete.

Som stöd till förvaltningschefen ska informationssäkerhetssamordnaren leda, samordna och följer upp det operativa arbetet inom den egna förvaltningen. Konkret innebär detta att informationssäkerhetssamordnaren ska utbilda och sprida kunskap om lokala rutiner bland medarbetare. Det innebär även att genomföra uppföljning av det lokala informationssäkerhetsarbetet.

Informationssäkerhetssamordnaren ska även, följa upp att informationsklassningar genomförs samt kontrollera hur kraven efterlevs. Häri ingår även att säkerställa att de skyddsåtgärder som följer av informationsklassningen, arbetas in i nya eller befintliga processer inom verksamheten.

Informationssäkerhetssamordnaren ska vara rådgivande till objektledaren och ska utifrån förvaltningens ansvar och behov, kravställa och samverka med objektledningen för att säkra upp att hela kedjan, från informationsklassning till införda säkerhetslösningar följer kommunens informationssäkerhetsregler.

Informationssäkerhetssamordnaren ska slutligen också vara kontaktpunkt för kommunens informationssäkerhetsansvarig samt regelbundet rapportera till denne.

Informationssäkerhetsarbetet inom ramen för pm3

En stor del av det praktiska arbetet med informationssäkerheten ska integreras i objekten, som är en del av pm3, kommunens styr- och samverkansmodell.

I objekten planeras och utförs den systematiska informations- och it-säkerheten på taktisk och operativ nivå, i enlighet med det systematiska årshjulet, i de system och verksamheter som representeras inom ett förvaltningsobjekt.

Objekten ska jobba riskbaserat och systematiskt med informations- och it-säkerhet, genom att årligen arbeta med riskanalyser och informationsklassningar.

I många fall levererar objekten it-tjänster med information från flera olika informationsägare, vilket också medför att ökat skyddsvärde. Objekten ansvarar för att samla in alla informationsägares krav för att definiera och genomföra lämpliga säkerhetsåtgärder.

Objekten ska bland annat:

- Inhämta krav från informationsägaren/informationsägarna
- Jobba systematiskt och riskbaserat
- Genomföra informationsklassningar och riskanalyser
- Ta fram och fullgöra handlingsplaner
- Regelbundet följa upp kravens efterlevnad

Med en förankrad styr- och samverkansmodell på plats finns det tydliga roller och ansvar som redan är bemannade. Genom att använda pm3-strukturen får kommunen naturligt in verksamhetens medverkan och krav i befintliga forum och sammanhang. Genom att lyfta in informationssäkerhet i objektens styrning, ledning och uppföljning blir det systematiska informationssäkerhetsarbetet en del av den löpande förvaltningen.

När objekten arbetar med sina riskanalyser torde såväl organisatoriska som tekniska sårbarheter komma att uppmärksammas och hanteras. Tekniska säkerhetsåtgärder är förenklat att betrakta som it-säkerhet och organisatoriska säkerhetsåtgärder är förenklat att betrakta som informationssäkerhet.

Slutsatser

För att ovanstående ska kunna implementeras i kommunens ledningssystem för informationssäkerhet ges informationssäkerhetsansvarig i uppdrag att, i samråd med it-säkerhetsansvarig, ta fram förslag på och genomföra erforderliga ändringar av informationssäkerhetshandboken och av berörda styrdokument samt vid behov föreslå nya styrdokument.

Informationssäkerhetsansvarig och it-säkerhetsansvarig ges vidare i uppdrag att vidareutveckla nya och befintliga roller och funktioner, utifrån de ansvar och mandat som tillkommer i och med förslaget.

Informationssäkerhetsansvarig och it-säkerhetsansvarig ansvarar för att såväl var och en för sig som gemensamt etablera de samverkansforum som beslutats.

Respektive förvaltningschef ges i uppdrag att utse minst en informationssäkerhetssamordnare per förvaltning. Funktionen ska finnas på plats från och med 1 mars 2024 och information om vem eller vilka som innehar uppdraget ska skickas till informationssäkerhetsansvarig, via juridikenhetens funktionsbrevlåda.

För att förslaget fullt ut ska kunna genomföras behöver kommunens pm3-modell vidareutvecklas. Det ansvaret åligger chefen för Utvecklings- och digitaliseringenheten.