VARA KOMMUN

REMISSVAR

2019-03-13

Remissvar – Policy och riktlinjer för informationssäkerhet

Bakgrund

I september 2018 tog IT-strategerna inom V6 initiativ till att ta fram nya gemensamma riktlinjer och policy för informationssäkerhet. Arbetet leds av en styrgrupp bestående av IT-strategerna samt VD för Göliska IT. Projektgruppen består av två personer; V6 informationssäkerhetssamordnare från Göliska samt en utvecklingsledare från Lidköpings kommun. Styrgruppen har nu godkänt de föreslagna dokumenten, och den 28 januari 2019 skickades de ut på remiss till kommunerna. Remissvaret ska ha inkommit till Lidköpings kansli senast den 30 april 2019.

I Vara har kansliavdelningen lett arbetet att ta fram ett gemensamt remissvar, tillsammans med representanter för förvaltningarna. Kommunens samtliga nämnder och personalutskott har getts möjlighet att yttra sig. Kommunstyrelsen sammanställer därefter nämndernas remissvar och avger ett, för Vara kommun, slutligt yttrande.

Yttrande

Om policyn

I arbetet med att ta fram en policy bör man hela tiden ha i åtanke vad en policy är tänkt att åstadkomma. En policy har främst två syften. Den ska vara en politisk viljeyttring, som visar vad kommunen eller kommunerna vill åstadkomma inom ett specifikt område. En policy ska även kunna förklara för medarbetarna hur kommunen tänker kring en viss fråga, och varför man gör det. I det här fallet bör policyn erbjuda en förklaring kring varför informationssäkerhetsarbetet är viktigt. Socialnämnden anser att det finns utrymme för förbättringar avseende båda syftena.

Den föreslagna policyn konstaterar att informationssäkerhetsarbetet ska bedrivas så att lagkrav på området uppfylls. Vidare konstateras att det ska finnas en lämplig organisation för informationssäkerhetsarbetet, att informationstillgångar ska kartläggas och incidenter rapporteras till tillsynsmyndigheter. Allt detta är rutiner som kan härledas från lagkrav. Att kommunerna ska uppfylla lagkrav är dock inte en självständig viljeyttring, Det är bra att detta nämns i policyn, men det utgör inte en policy i sig.

På slutet nämns att ”informationssäkerhetsarbetet ska bidra till effektivt stöd i kärnverksamheten”. Detta är mer av en självständig viljeyttring, varför nämnden ser behov av att denna del utvecklas. Örebros policy är ett bra exempel att studera vad gäller detta. I deras policy konstateras att informationssäkerhet inte har något egenvärde, utan det viktiga är hur det kan bidra till andra mål.

POSTADRESS	BESÖKSADRESS	TEL VÄXEL	FAX	E-POST	HEMSIDA
Vara kommun	St. Torget 8	0512-310 00	0512-313 10	vara.kommun@vara.se	www.vara.se
534 81 VARA	VARA				

Efter detta anges de positiva effekter som Örebro kommun förväntar sig få ut av sitt informationssäkerhetsarbete. Socialnämnden anser att policyn med fördel kan koppla samman informationssäkerhetsarbetet med gemensamma mål inom V6. Exempelvis skulle man kunna fastslå att:
Informationssäkerhetsarbetet ska bedrivas så att det underlättar effektiviseringar av kommunernas verksamheter samt främjar digital inkludering bland kommuninvånarna.
Sådana ställningstaganden visar vad kommunerna vill åstadkomma med informationssäkerhetsarbetet bortom lagkraven, och hjälper medarbetare att förstå vinsterna med god informationssäkerhet. Policyförslaget slår fast målsättningen att ”Kommunen har en organisation med lämplig kompetens och relevanta roller för ett systematiskt informationssäkerhetsarbete”. Socialnämnden anser att policyn bör förtydliga ansvarsfördelningen inom V6 och inom varje kommun, dock utan att gå in på detaljnivå. I organisationer med en dåligt fungerande informationssäkerhetskultur läggs ofta allt ansvar för informationssäkerhet på IT-avdelningen och informationssäkerhetssamordnaren. Socialnämnden ser möjligheter i att en gemensam policy inom V6 kommunerna kan förtydliga att informationssäkerhet är ett gemensamt ansvar hos alla medarbetarna. Samt med förtydligande att kommunernas alla ledningar har det yttersta ansvaret för informationssäkerheten och det förebyggande arbetet. Policyförslaget fastslår förvisso att det ligger på alla medarbetare att följa policyn, men att medarbetare ska följa policyer får ses som självklart. Det socialnämnden efterfrågar är en lista på olika roller inom informationssäkerhetsarbetet, som i detta (ej uttömmande) exempel:

***Medarbetare**:*
Varje medarbetare ansvarar för att följa denna policy och riktlinjer kring informationssäkerhet. Vidare har man ett ansvar att uppmärksamma brister och incidenter och rapportera dessa till …

Ledningar:
Ledningar i form av kommunfullmäktige, kommunstyrelse och nämnder har det yttersta ansvaret för informationssäkerheten inom sina ansvarsområden …

Verksamhetsansvariga:
Verksamhetsansvariga är ansvariga för informationssäkerheten inom sin verksamhet, och ansvarar för att medarbetare har den kunskap och förståelse för informationssäkerhet som behövs …

Informationssäkerhetssamordnaren:
Har det övergripande ansvaret för att leda och utveckla informationssäkerhetsäkerhetsarbetet …
…osv

Exempel på kommuner som på ett mycket tydligt sätt har spaltat upp de olika rollernas ansvar i sina policyer är Örebro och Eksjö. Även Arvikas, Linköpings och Hudiksvalls policyer kan vara värda att hämta inspiration från.

Socialnämnden anser att språket i policyn behöver förenklas och förtydligas. Policyn ska kunna läsas och förstås av alla kommunens medarbetare och förtroendevalda, oavsett bakgrund och utbildningsnivå. En exempelmening

från policyutkastet är det mycket viktiga konstaterandet: ”Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.” Här skulle man kunna förtydliga och ange exempel på både digitala och icke-digitala informationstillgångar. Med en lägre abstraktionsnivå minskar risken att policyn inte implementeras i alla verksamheter. Att genomgående ha ett vi-tilltal är också något som bör övervägas för att komma närmare läsaren. Örebros och Eksjös policyer är bra exempel på lättillgängligt språkbruk.

I de föreslagna riktlinjerna anges att styrdokument kring informationssäkerhet ska tas fram och integreras i kommunens ledningssystem. Socialnämnden anser att detta stycke passar bättre att ha med i policyn. Detsamma gäller riktlinjernas sektion om ”Grundläggande krav och rekommendationer för informationssäkerhet”. Detta diskuteras mer i granskningen av riktlinjerna.

I korthet förordas att policyn skrivs om med följande tillägg och ändringar:

- Tydligare förklaring av vad V6-kommunerna ser för vinster med god informationssäkerhet – sammankoppla informationssäkerheten med andra mål och visioner!
- Mer information om ansvarsfördelning, tydliggör att alla chefer och medarbetare har ett ansvar för informationssäkerheten. Spalta upp de olika rollerna.
- En översyn av språkbruket med fokus på att dokumentet ska vara lättförståeligt för alla kommunens medarbetare.
- Flytta över sektionerna ”Grundläggande krav och rekommendationer för informationssäkerhet” och ”Styrande dokument” från riktlinjerna till policyn.

Om riktlinjerna

Riktlinjer skiljer sig från policyer då de ska fungera som föreskrifter som ger konkret vägledning till chefer och medarbetare i det dagliga arbetet. I det här fallet ska medarbetare kunna vända sig till riktlinjerna för att förstå hur de ska agera för att leva upp till kraven på informationssäkerhet. Socialnämnden anser att de föreslagna riktlinjerna i sin nuvarande form är för kortfattade och generella för att erbjuda ett sådant stöd. Således krävs en omfattande utökning och specificering av riktlinjerna för att de ska vara relevanta att anta. Det anges förvisso i remissen att de ska kompletteras med verksamhetsspecifika riktlinjer, men socialnämnden ser ingen anledning att anta riktlinjer som är så generella att de inte kan fungera som stöd till verksamheterna.

Vad gäller innehållet i förslaget till riktlinjer anser socialnämnden att de tre första sektionerna, ”Inledning”, ”Lagstiftning” och ”Intressenter” är passande att ha med i början av riktlinjerna för att ge en bakgrund till de efterföljande rekommendationerna. I den utvidgade versionen av riktlinjerna som socialnämnden rekommenderar bör även inledningen utökas och kompletteras med en innehållsförteckning. Detta för att ge läsaren en överblick över dokumentet och möjlighet att hitta relevant sektion. Riktlinjernas två sista sektioner, ”Grundläggande krav och rekommendationer för informationssäkerhet” och ”Styrande dokument” tar upp viktiga aspekter av informationssäkerhetsarbetet. De är dock för generellt skrivna för att passa

som riktlinjer, och socialnämnden ser att de med fördel kan införlivas i policydokumentet. Språkbruket bör då ses över på samma sätt som för övriga delar av policyn.

I den medföljande remissen anges att antagandet av policyn och riktlinjerna innebär att alla tidigare antagna styrdokument i V6 gällande informationssäkerhet ska upphävas. Vara kommun har sedan tidigare styrdokument som ”Riktlinjer – IT-säkerhet för användare” (se bilaga 2).

Dessa är i behov av uppdatering då de antogs innan kommunen gick med i Göliska, och därmed hänvisar de till kommunens gamla IT-avdelning. De diskuterar dock på en detaljerad nivå hur medarbetare bör agera gällande exempelvis e-post, lösenord och hemarbete. Ett annat exempel gäller socialnämnden som på sammanträde i februari (SN 21§) beslutade om ett reviderat dokument med detaljerade riktlinjer beträffande informationssäkerhet för sin verksamhet. Ifall dessa detaljerade riktlinjer skulle ersättas av de nu föreslagna riktlinjerna vore det direkt kontraproduktivt ur informationssäkerhetssyfte. Socialnämnden anser att detta inte är en godtagbar ordning.

För att riktlinjerna ska fylla en funktion anser socialnämnden att ett minimikrav är att de behandlar samma områden som nuvarande riktlinjer. Detta skulle kunna åstadkommas genom att nuvarande riktlinjer inom de olika kommunerna jämkas och sammanfogas. De förslag som listas i Bilaga 1 bör då också beaktas. Socialnämnden anser att antagande av riktlinjer bör avvaktas. En omarbetning av policyn i linje med socialnämndens rekommendationer innebär att den i sig kommer att omfatta mer än de nuvarande förslagen på policy och riktlinjer. Arbetsgruppen för då fokusera på att ta fram gemensamma riktlinjer för V6 som kan tala om hur verksamheterna ska arbeta för att uppnå det policyn anger. Två dokument som är värda att studera inför detta arbete är Örebros ”Riktlinjer för informationssäkerhet” och Uddevallas ”Regler för informationssäkerhet”.

I korthet förordar socialnämnden att arbetet med riktlinjerna görs om enligt följande:

- Sektionerna ”Grundläggande krav och rekommendationer för informationssäkerhet” och ”Styrande dokument” flyttas från riktlinjerna till policyn.
- I första hand bör riktlinjerna arbetas om från grunden för att erbjuda ett tydligt regelverk för medarbetare gällande informationssäkerhet.
- I andra hand bör riktlinjerna skrivas om genom att kommunernas nuvarande riktlinjer jämkas och sammanfogas, tillsammans med rekommendationer kring de punkter som tas upp i Bilaga 1.
- Nyligen antagna förvaltningsspecifika riktlinjer ska inte upphävas, men bör vid behov uppdateras för att stämma överens med de nya övergripande riktlinjerna.
- De nu föreslagna riktlinjernas tre första sektioner kan med fördel infogas i de nya riktlinjerna.