Datum
2022-02-16

Tjänsteskrivelse

Vår referens
Anton Wikman
Utvecklingssekreterare
anton.wikman@malmo.se

Antagande av nya riktlinjer för informationssäkerhet i Malmö stad
STK-2021-1717

Sammanfattning

I samband med att Malmö stads informationssäkerhetsarbete granskandes 2018 beslutade kommunstyrelsen i sitt yttrande till revisorskollegiet (STK-2018-1064) att ge stadskontoret i uppdrag att genomföra en större revidering av befintligt styrdokument-*Riktlinjer och anvisningar för informationssäkerhet i Malmö stad.* Som ett komplement till den genomförda granskningen beslutade stadskontoret att under 2019 genomföra en nulägesuppföljning av informationssäkerhetsområdet. Uppföljningens huvudsyfte var att undersöka informationssäkerhetssamordnarens förutsättningar att efterleva gällande riktlinje. Resultatet redovisades för stadskontorets ledningsgrupp i januari 2020, se ärende STK-2020-523.

I väntan på att nulägesuppföljningen skulle färdigställas genomfördes endast mindre korrigeringar av riktlinjen 2019 med ambitionen att ett nytt styrdokument skulle vara på plats under 2020, se ärende STK-2019-588. Dröjsmålet att ta fram en ny riktlinje beror dels på pågående pandemi, samt stadskontorets vilja att vänta in och beakta utfallet av de nya IT- och digitaliseringsriktlinjer som antogs i början av 2021 samt att den nya IT-organisationen skulle etablera sig hos serviceförvaltningen.

Stadskontoret har nu arbetat fram ett förslag till ny riktlinje. Förslaget innebär ett helt nytt styrdokument vars övergripande syfte är att på strategisk nivå tydliggöra ansvar, målsättning och arbetssätt avseende informationssäkerhetsarbetet i Malmö stad.

Förslaget innebär i korthet att:

- Nuvarande riktlinjer och anvisningar för informationssäkerhet i Malmö stad upphör att gälla.
- Ny dokumentstruktur etableras med en väsentligt nedkortad riktlinje som fastställer ansvar, målsättning och arbetssätt på strategisk nivå emedan detaljkrav och vägledningar flyttas till underliggande anvisningar, regler och rutiner.
- Kommunstyrelsens och övriga nämnders ansvar tydliggörs för att främja det systematiska informationssäkerhetsarbetet och skapa ökad tydlighet kring ansvar och mandat.
- Ny styrning avseende uppföljning och aktivitetsplanering.

Frågeställningar

Stadskontoret välkomnar synpunkter på hela riktlinjen, dess intentioner och förväntade effekter. Följande frågeställningar har identifierats som särskilt värdefulla att belysa under remissen:

- Är riktlinjen tydlig avseende nämndens ansvar och uppdrag?
- Är samordnarens roll, ansvar och uppdrag tillräckligt tydlig?
- I vilken omfattning kommer förslaget att påverka nämndens ansvarsområde?
- Vilket stöd behöver nämnden från kommunstyrelsen för att implementera riktlinjerna?
- Innebär förslaget några ekonomiska konsekvenser för nämnden? I så fall i vilken omfattning?

Förslag till beslut
Kommunstyrelsens arbetsutskott föreslås besluta

1. Kommunstyrelsens arbetsutskott skickar, utan eget ställningstagande, förslag till *Riktlinjer för informationssäkerhet i Malmö stad* på remiss till samtliga nämnder med svar till stadskontoret senast den 2 maj 2022.

Beslutsunderlag
- G-Tjänsteskrivelse KSAU 220221 Antagande av nya riktlinjer för informationssäkerhet i Malmö stad; remiss
- Förslag på nya riktlinje för informationssäkerhet i Malmö stad

Beslutsplanering
Kommunstyrelsens arbetsutskott 2022-02-21
Kommunstyrelsens arbetsutskott 2022-05-30
Kommunstyrelsen 2022-06-07

Beslutet skickas till
Samtliga nämnder

Ärendet
Nuvarande riktlinjer togs fram 2013 (se ärende STK-2013-224) och har sedan dess reviderats ungefär vartannat år för att passa verksamhetens behov. I samband med granskning av Malmö stads informationssäkerhetsarbete 2018 beslutade kommunstyrelsen i sitt yttrande till revisorskollegiet (STK-2018-1064) att ge stadskontoret i uppdrag att genomföra en större översyn och revidering av befintligt styrdokument-*Riktlinjer och anvisningar för informationssäkerhet i Malmö stad.*

Som ett komplement till den genomförda granskningen beslutade stadskontoret att under 2019 genomföra en nulägesuppföljning av informationssäkerhetsområdet. Uppföljningens huvudsyfte var att undersöka informationssäkerhetssamordnarens förutsättningar att efterleva gällande riktlinje. Resultatet redovisades för stadskontorets ledningsgrupp i januari 2020, se ärende STK-2020-523.

I väntan på att nulägesuppföljningen skulle färdigställas genomfördes endast mindre korrigeringar av riktlinjen 2019 med ambitionen att ett nytt styrdokument skulle vara på plats under 2020, se ärende (STK-2019-558). Dröjsmålet att ta fram en ny riktlinje beror dels på pågående pandemi samt stadskontorets vilja att vänta in och beakta utfallet av de nya IT- och digitaliseringsriktlinjer som antogs i början av 2021 samt att den nya IT-organisationen skulle etablera sig hos serviceförvaltningen.

1. Behovet att arbeta med informationssäkerhet i Malmö stad

Stora mängder information skapas och behandlas dagligen av Malmö stads medarbetare och verksamheter. Information finns överallt och bristande informationssäkerhet innebär alltid sårbarheter och inte sällan även lagbrott. I värsta fall kan både viktig och känslig information hamna i orätta händer, vilket kan bli mycket kostsamt och påverka medborgarnas förtroende för Malmö stad.

Informationssäkerhetens huvudsyfte är, enkelt uttryckt, att Malmö stad ska ha full koll på sin informationshantering och att all information oavsett form eller kanal ska hanteras på ett korrekt och säkert sätt utifrån gällande lagar, föreskrifter och interna krav. För att säkerställa detta har staden en process för informationsklassificering. Processen kan användas av stadens alla verksamheter och innebär en riskbedömning av verksamhetens informationshantering. Klassningsprotokollet fungerar som underlag vid utformning och kravställning av säkerhetsåtgärder och avgör hur informationen ska skyddas så den inte kommer någon obehörig tillhanda, alltid är korrekt och finnas tillgänglig när den behövs.

Behovet att tillämpa klassificering och införa de krav som ställs på verksamheterna utifrån informationssäkerhet är avgörande för att säkra stadens informationshantering. Detta gäller framför allt den digitala informationen där allt fler IT-system och digitala tjänster öppnar upp nya hotbilder och sårbarheter i stadens informationshantering. Kraven på högre informationssäkerhet märks även utifrån instiftandet av bland annat patientdatalagen, NIS-lagstiftningen, säkerhetsskyddslagen och dataskyddsförordningen som alla ställer krav eller förutsätter ett strukturerat och organiserat informationssäkerhetsarbete.

Malmö stad måste arbeta mer aktivt för att säkerställa att informationssäkerhet alltid beaktas när våra verksamheter hanterar information. Genom att aktivt tillämpa processen för klassificering och därmed avgöra informationens skyddsvärde så kan vi tillsammans arbeta för att höja hela stadens säkerhetsnivå och skydda vår information på ett tillräckligt och avvägt sätt.

2.Förändringar gentemot befintligt styrdokument

För att visa vilka förändringar som gjorts i och med föreslagen riktlinje redovisas här nedan tre förändringsområden som fångar den utveckling som kan förväntas av att den nya riktlinjen och underliggande styrdokument implementeras i staden.

2.1 Övergripande ansvar och styrning

Flera revisioner har påpekat att nuvarande riktlinje inte nog tydligt definierar vem som har ansvar för stadsövergripande styrning och ledning av stadens arbete med informationssäkerhet samt vem som egentligen ansvarar för att innehållet i riktlinjen implementeras i stadens verksamheter.

Med ovanstående brister i åtanke har det nya styrdokumentet lyft fram ansvar som ett eget kapitel med syftet att synliggöra de olika ansvaren och gränsdragningarna däremellan. Nedan ges en kortfattad förklaring hur den nya riktlinjen reglerar den stadsövergripande, strategiska styrningen gällande informationssäkerhet, samt vem som bär ansvaret för implementering av beslutade styrdokument i stadens verksamheter.

I kommunstyrelsens reglemente framgår det att styrelsen ”ansvarar för det övergripande arbetet med informationssäkerhet”. Denna skrivelse ska läsas i kontexten av hela reglementet som fastslår att kommunstyrelsen är kommunens ledande politiska förvaltningsorgan och har i uppdrag att **leda**, **samordna** och **ha uppsikt över** kommunens verksamheter.

Sammantaget ska kommunstyrelsen;

- Leda och samordna förvaltningen av kommunens angelägenheter och ha uppsikt över övriga nämnders verksamhet (ledningsfunktion). Styrelsen ska också ha uppsikt över kommunal verksamhet som bedrivs i kommunala företag, stiftelser och kommunalförbund

- Utifrån ett helhetsperspektiv leda kommunens verksamhet genom att utöva en samordnad styrning och leda arbetet med att ta fram nämndsövergripande styrdokument för kommunen (styrfunktion)

- Följa de frågor som kan inverka på kommunens utveckling och ekonomiska ställning och fortlöpande i samråd och samverkan med nämnderna följa upp de fastställda målen och återrapportera till fullmäktige (uppföljningsfunktion)

Kommunstyrelsen ansvarar också för beslut om samordning mellan nämnderna, gränsdragning mellan nämndernas kompetens och för att en effektiv och ändamålsenlig organisation upprätthålls i den kommunala verksamheten. Stadskontoret som styrelsens förvaltning har genom sitt reglemente givits ett centralt, stadsövergripande ansvar att sätta ramarna och de övergripande processerna inom vilket allt informationssäkerhetsarbete i Malmö stad ska bedrivas.

I föreslagen riktlinje tydliggörs detta ansvar genom att fastslå att kommunstyrelsen beslutar om riktlinjen samt att stadskontoret har det övergripande strategiska ansvaret i staden och ansvarar för att leda, samordna och följa upp stadens arbete inom området. I praktiken innebär de nya skrivningarna i riktlinjen endast ett förtydligande av kommunstyrelsens och stadskontorets befintliga uppdrag.

När det gäller ansvaret för implementering av beslutade styrdokument i stadens verksamheter bygger föreslagen riktlinje på stadens ordinarie styr- och ansvarsprincip. Nämligen att varje nämnd är ansvarig för den verksamhet som bedrivs inom ramen för sitt ansvarsområde och är därmed även ansvarig för att gällande krav avseende informationssäkerhet efterlevs inom sin förvaltning. Ovanstående ansvarsfördelning mellan kommunstyrelsen och stadens nämnder följer även befintlig trygghets- och säkerhetspolicy som sätter ramarna för hur allt trygghets- och säkerhetsarbete ska bedrivas.

2.2 Förvaltningsledningens ansvar

Även om varje nämnd är ytterst ansvarig för allt inom sin egen förvaltning är det i praktiken förvaltningens ledningsgrupp och dess förvaltningsdirektör som tillser att de krav som åligger förvaltningens verksamhet efterlevs.

Ledningens kunskap och förståelse för informationssäkerhet är viktigt för att ledningen ska kunna ta ställning och fatta välgrundade beslut. Vilket i sin tur är avgörande för att informationssäkerhetsarbetet ska få genomslag i verksamheten. För att kunna åstadkomma detta behöver ledningen få både information i form av uppföljning samt möjligheten att ta ställning till frågor på området genom att åtgärdsförslag lyfts för beslut. För att både uppföljningsresultat och besluts-

underlag ska komma ledningen till handa ska varje förvaltningsledning utifrån föreslagen riktlinje utse en informationssäkerhetssamordnare i sin förvaltning.

2.3 Informationssäkerhetssamordnarens roll och ansvar

I varje förvaltning ska det finnas en utpekad informationssäkerhetssamordnare. Rollen ansvarar för att samordna förvaltningens interna informationssäkerhetsarbete och ska arbeta långsiktigt och verksamhetsövergripande för att informationssäkerhet ska integreras i förvaltningens verksamheter och processer. Rollen ansvarar även för att:

- Följa upp förvaltningens informationssäkerhetsarbete.
- Rapportera till förvaltningsledningen.
- Vara kontaktperson till Malmö stads strategiska samordnare
- Vara den egna förvaltningens representant i Malmö stads interna informationssäkerhetssamordnarnätverk.
- Kunna leda och bistå med kompetens vid genomförande av informationsklassificering.
- Kunna leda och bistå med kompetens vid riskanalyser inom ramen för riktlinjens och anvisningarnas omfattning.

Utsedd person är stadskontorets motpart inom området och kommer att inkluderas i kommunens övergripande strategiska arbete samtidigt som rollen ska arbeta tillsammans med motsvarande roller inom samtliga förvaltningar för att Malmö stad ska uppnå ett samordnat och systematiskt arbete med informationssäkerhet. För att uppnå en god förmåga i staden krävs att samordnaren ges utrymme att arbeta strategiskt och tillsammans över förvaltningsgränserna med utrymme för innovation, omvärldsbevakning, och kunskapsutveckling. Stadskontoret kommer att ge rollen kontinuerlig kompetensutveckling och stöttar vid behov förvaltningarna med kunskapsunderlag inför rekrytering samt introduktion av rollen. Förvaltningsledningen måste dock tillse att personen får tillräckligt med utrymme och tid för att axla uppdraget.

Rollen ska utifrån ovanstående bakgrund dimensioneras i förhållande till förvaltningens storlek, typ av verksamhet, samlade informationshantering och riskbild. Som vägledning vill stadskontoret framhäva nulägesuppföljningen från 2019, se ärende STK-2020-523 samt påminna att stadskontoret gärna ger vägledning och stöd till förvaltningarna vid utredning av resursbehov.

2.4 Uppdragets förutsättningar

För att lyckas med uppdraget krävs förståelse för området och utrymme till delaktighet och kunskapsutveckling. Detta innebär aktivt deltagande i det stadsgemensamma arbetet samtidig som personen ges möjlighet till utbildning och omvärldsbevakning. Att arbeta med informationssäkerhet innebär att fokus ligger på att analysera verksamhetens informationshantering utifrån rådande risk och hotbilder samt övergripande förståelse för påverkande lagar, regelverk, interna krav samt den tekniska utvecklingen. Samordnarens kunskap om bland annat informationsklassificering och riskanalyser ska hjälpa förvaltningen att analysera och ställa krav på nya och etablerade processer, informationsmängder och IT-system så de upprätthåller rätt nivå av skydd baserat på informationens skyddsvärde och riskbild.

Var i förvaltningsorganisationen som samordnaren är placerad har betydelse, vilket har visat sig vid genomförda revisioner och nulägesuppföljningar. För att kunna verka effektivt i sin roll bör samordaren vara placerad nära ledningen. Enligt MSBs metodstöd kan lämpliga placeringar vara hos säkerhet, juridik, kvalitet/uppföljning samt strategisk-IT. I det fall rollen placeras inom IT eller digitalisering ska ledningen vara medveten om att det kan leda till intressekonflikter. Detta

kan förekomma eftersom uppdraget innebär en granskande funktion samt att agera kravställare gentemot den digitala informationshanteringen och därmed även förvaltningens IT- och digitaliseringsinitativ. Det viktigaste i valet av organisatorisk placering är att den egna ledningen gjort ett medvetet val, baserat på verksamhetens behov och där samordnarrollen ges de förutsättningarna som krävs för att kunna bedriva ett effektivt och ändamålsenligt arbete.
När samordnarrollen är tillsatt behöver dess uppdrag göras känd inom den egna verksamheten. Detta är avgörande för att samordnaren i god tid ska få information och involveras i förvaltningens olika arbeten och uppdrag. Ett exempel på sådana områden är upphandling av IT-system och digitala tjänster. Inom upphandlingsprocessen är genomförande av informationsklassificering en grundförutsättning för att kunna ställa rätt krav utifrån informationens skyddsvärde.

2.5 Förväntad effekt

Föreslagna riktlinjer förväntas tydliggöra ansvaret på alla nivåer i organisationen och ge ökad tydlighet avseende stadskontorets och kommunstyrelsens ansvar för den stadsövergripande, strategiska styrningen. Föreslagen styrmodell skiljer sig inte avsevärt från hur befintlig styrning inom området har sett ut sedan 2013 men förhoppningen är att den nya riktlinjen med sitt strategiska fokus ska leda till att de olika ansvaren synliggörs. Avgörande för att denna styrmodell ska fungera är att förvaltningarnas samordnare ges rätt förutsättningar för att kunna utföra sin roll och att varje förvaltning (och därmed staden som helhet) ska kunna bedriva ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

3. Ny dokumentstruktur

Föreslagen riktlinje innebär en helt ny dokumentstruktur med en nedkortad riktlinje från nuvarande 47 till 11 sidor, exklusive bilagor. Den nya riktlinjens fokus är att fastställa ansvar, målsättning och arbetssätt på strategisk nivå. Alla relevanta detaljkrav och vägledningar från nuvarande styrdokument kommer att ses över och flyttas till underliggande anvisningar, regler och rutiner som beslutas på tjänstepersonsnivå. I de fall verksamhetsspecifika rutiner saknas är det upp till respektive förvaltning att ta fram kompletterande rutiner utifrån identifierat behov.

Den nya dokumentstrukturen har tillkommit utifrån tre tydliga behov;

- Lyfta fram och synliggöra ansvar samt förtydliga den strategiska styrningen av informationssäkerhetsområdet.
- Nödvändigheten att enkelt kunna revidera detaljkraven för att harmonisera med förändringar i lagar, interna regelverk och den tekniska utvecklingen.
- Harmonisera med gällande ansvarsfördelning och organisering av informations- och IT-säkerhetsfrågorna där detaljstyrning och kravställning av Malmö stads digitala informationshantering flyttats från stadskontoret och nu ligger hos IT- och digitaliseringsavdelningen(ITD)- serviceförvaltningen.

Den nya dokumentstrukturen ser ut på följande sätt:

3.1 Förväntad effekt

Genom framtagandet av en ny, nedkortad riktlinje är förhoppningen att informationssäkerhetsområdets strategiska styrning ska bli tydliggjord i syfte att klargöra ansvar, målsättning och stadsövergripande arbetssätt. Genom att lyfta ner detaljstyrningen till underliggande anvisningar som beslutas på tjänstepersonsnivå behöver anvisningarna inte (såsom nuvarande riktlinje) upp för beslut i kommunstyrelsen vid varje korrigering eller förändring. Anvisningarna kan därmed snabbt revideras vilket säkerställer att deras innehåll enklare kan hållas aktuellt i förhållande till gällande lagstiftning och den tekniska utvecklingen.

De förändringar som skedde 2021 avseende stadskontorets uppdrag där hela före detta IT-enheten förflyttades till serviceförvaltningen i en ny organisation innebar att ansvaret avseende den digitala säkerheten försvann från stadskontoret. För att den nya dokumentstrukturen ska harmonisera med hur staden valt att organisera och fördela uppdrag inom IT-säkerhet och digital informationshantering är förslaget att ansvaret för att ta fram en anvisning för dessa områden ska ligga på ITD-serviceförvaltningen.

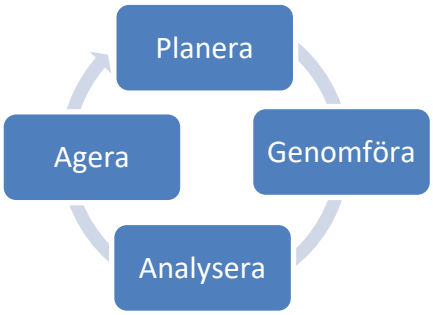
Skapandet av anvisningar under riktlinjen möjliggör för mer ingående vägledning vid implementering av kraven, något som gällande riktlinje saknar då den redan i befintlig form anses för omfattande och komplex. Den nya dokumentstrukturen förväntas innebära en tydligare styrning och mer praktiskt användbara anvisningar som inte bara ställer krav utan även ger viss vägledning för hur och var de ska implementeras i verksamheten.

4.Uppföljning

Föreslagen riktlinje innebär en ny styrning när det gäller uppföljning och rapportering av stadens informationssäkerhetsarbete. Den nya styrningen avseende uppföljning har uppkommit utifrån behovet att uppföljning måste bli en naturlig och självklar del av allt arbete med informationssäkerhet. Till skillnad från dagens styrdokument så ställer nya riktlinjen krav på att samordnaren årligen ska rapportera till den egna förvaltningsledningen samt att den strategiska samordnarrollen, placerad på stadskontoret årligen ska göra en stadsövergripande sammanställning och rapportera resultatet till stadens ledningsgrupp.

Uppföljningens resultat ska vara sammankopplad med föreslagna målområden för informationssäkerhet samt de övriga kraven som ställs enligt föreslagen riktlinje. I riktlinjen tydliggörs även uppföljning som en uttalad aktivitet som alltid ska vidtas vid genomförande av alla åtgärder kopplat till informationssäkerhet. Detta arbetssätt säkerställs genom att riktlinjen ställer krav på att allt informationssäkerhetsarbete ska bedrivas systematiskt baserat på följande styrning;

- **Planera**: Utifrån lagstiftning, styrdokument, informationsklassificeringar, incidenter och riskbedömningar identifiera och planera att införa säkerhetshöjande åtgärder.
- **Genomföra**: Genomför planerade åtgärder.
- **Analysera**: Utvärdera införandet. Kontrollera att syftet med åtgärderna är uppfyllt.
- **Agera**: Ta fram förslag på nya säkerhetshöjande åtgärder.



4.1 Förväntad effekt

Förhoppningen är att det nya sättet att arbeta med uppföljning ska leda till en mer systematisk, riskbaserad och långsiktig uppföljningsprocess där syfte och kvalitén av utförda åtgärder ständigt följs upp och utvärderas. Därför ställer riktlinjen krav på att uppföljning ska ske årligen på både på nämnds- och stadsövergripande nivå och samtidigt förtydliga hur uppföljning ska ske. Genom att koppla samman uppföljningsprocessen med riktlinjens målområden och övriga krav är målet att synliggöra informationssäkerhetsarbetets utveckling över tid.

Resultatet av uppföljningen är tänkt att användas som underlag för planering av aktiviteter på både nämnds- och stadsövergripande nivå och samtidigt ge vara ett underlag för vilka åtgärder som behöver prioriteras. Avsikten är att underlätta för förvaltningarna att komma igång med det systematiska arbetet. Samt att kunna leverera både underlag och rekomendatoner till den egna förvaltningsledningen att ta ställning kring. Det nya sättet att arbeta med uppföljning ska förhoppningvis leda till att ledningsgruppen i varje förvaltning får fördjupad kunskap och insikt på området samtidigt som stadens ledningsgrupp via den stadsövergripande sammanställningen får ökad kontroll och insyn i stadens arbete som helhet.

5. Vägen framåt

Föreslagen riktlinje förväntas ge informationssäkerhetsområdet en behövlig omstrukturering avseende dess övergripande styrning och öppnar upp för nya arbetssätt där ansvar, mål och stadsövergripande processer blir tydliggjorda. Samtidigt är framtagandet av en ny riktlinje bara början på ett flerårigt utvecklingsarbete som alltid ska upprätthållas. Informationssäkerhetsarbetet i staden har således inget slut utan är ett systematiskt arbete som innebär ständig förbättring och utveckling över tid. Föreslagen riktlinje medför en höjning av ambitionsnivån inom området där bland annat etablerandet av en stadsövergripande uppföljnings- och aktivitetsplaneringsprocess för hela staden ska synliggöra och konkretisera hur vi arbetar med frågorna. Ett nytt styrdokument och nya processer åstadkommer däremot inte förändring av sig själv. För att Malmö stad ska höja sin förmåga att arbeta med informationssäkerhet krävs resurser. Tillsättandet av en infosäk-samordnare i varje förvaltning som får utrymme att utföra och växa i sin roll och uppdrag är en grundförutsättning för stadens utveckling inom området.

6. Förankring

Som ett led i arbetet med att ta fram den nya riktlinjen har informationssäkerhetssamordnarna i varje förvaltning involverats i arbetet. Under riktlinjens framtagning har utkast redovisats för funktioner inom IT, juridik, verksamhetsuppföljning och dataskydd. Inhämtade synpunkter har efter bedömning reviderats in i förslaget, och därefter granskats ytterligare en gång av representanter från juridiska avdelningen innan beslutsprocessen tog vid. Hänsyn har också tagits till de genomförda revisioner och uppföljningar som skett mellan åren 2018-2021 och de förbättringsåtgärder som framkommit vid dessa. Vidare har intryck hämtats från Stockholms Stads, Göteborgs Stads och Region Skånes arbetssätt.

Ansvariga

Micael Nord Näringslivsdirektör
Magdalena Bondeson Sektionschef
Andreas Norbrant Stadsdirektör