Malmö stad
Kommunstyrelsen

Protokollsutdrag

Sammanträdestid	2022-06-07 kl 13:00-15:05
Plats	Sessionssalen, stadshuset
Utses att justera	Helena Nanne
Justeringen	2022-06-17
Protokollet omfattar	§232

Underskrifter

Sekreterare ..... Pernilla Mesch

Ordförande ..... Roko Kursar .....

Justerande ..... Helena Nanne .....

Beslutande ledamöter

Roko Kursar (L) (1:e vice ordförande)
Helena Nanne (M) (2:e vice ordförande)
Andréas Schönström (S)
Rose-Marie Carlsson (S)
Mubarik Mohamed Abdirahman (S)
Stefana Hoti (MP)
Emma-Lina Johansson (V)
Håkan Fäldt (M)
John Roslund (M)
Anton Sauer (C)
Magnus Olsson (SD)
Anders Olin (SD)
Anders Rubin (S) ersätter Katrin Stjernfeldt Jammeh (S) (Ordförande)

Ej tjänstgörande ersättare

Nils Anders Nilsson (S)
Frida Trollmyr (S)
Sara Wettergren (L)
Janne Grönholm (MP)
Anders Skans (V)
John Eklöf (M)
Tony Rahm (M)
Josefin Anselmsson Borg (M)
Martin Molin (C)
Nima Gholam Ali Pour (SD)
Rickard Åhman Persson (SD)

Övriga närvarande

Carina Nilsson (S) (Kommunfullmäktiges ordförande)
Simon Christander (L) (Kommunalråd)
Andreas Norbrant (Stadsdirektör)
Pernilla Mesch (Sekreterare)
Tomas Bärring (Chefsjurist)
Magdalena Bondeson (Sektionschef)
Julia Campbell (Nämndsekreterare)
Martin Ljungberg (Nämndsekreterare)
Per-Erik Ebbeståhl (Avdelningschef)
Niklas Sjöqvist (Presschef)
Johanna Juhlin (HR-direktör)
Ann Andersson (Budgetchef)
Anna Westerling (Ekonomidirektör)
Jonas Rosenkvist (Avdelningschef)
Micael Nord (Näringslivsdirektör)
Mats Holmström (Kommunikationsdirektör)
Claes Ramel (Finanschef)

§ 232 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.

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 informationssäkerhet i Malmö stad. Förslaget har varit på remiss hos samtliga förvaltningar vilket föranlett vissa mindre ändringar och förtydliganden i riktlinjen.

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 ett riskbaserat och systematiskt informationssäkerhetsarbete med ökad tydlighet avseende ansvar och mandat.
- Ny styrning avseende uppföljning och aktivitetsplanering.

Beslut

Kommunstyrelsen beslutar

1. Kommunstyrelsen godkänner föreslaget styrdokument Malmö stads riktlinjer för informationssäkerhet att gälla från 1 november 2022.

2. Kommunstyrelsen upphäver styrdokumentet Riktlinjer och anvisningar för informationssäkerhet i Malmö stad från och med 31 oktober 2022.

Beslutet skickas till

Samtliga nämnder

Beslutsunderlag

- Förslag till beslut KSAU 220530 §355
- G-Tjänsteskrivelse KSAU 220530 Antagande av nya riktlinjer för informationssäkerhet i Malmö stad

- Malmö stads riktlinjer för informationssäkerhet
- Stadsbyggnadsnämnden beslut 220427 § 132
- Remissvar från stadsbyggnadsnämnden
- Gymnasie- och vuxenutbildningsnämnden beslut 220429 § 61
- Remissvar från gymnasie- och vuxenutbildningsnämnden
- Överförmyndarnämnden beslut 220425 § 28
- Remissvar från överförmyndarnämnden
- Kulturnämnden beslut 220420 § 44
- Remissvar från kulturnämnden
- Servicenämnden beslut 220426 § 46 med Särskilt yttrande (M+C)
- Remissvar från servicenämnden
- Hälsa-, vård- och omsorgsnämnden beslut 220429 § 62
- Remissvar från hälsa-, vård- och omsorgsnämnden
- Grundskolenämnden beslut 220420 § 54
- Remissvar från grundskolenämnden
- Tekniska nämnden beslut 220426 § 110 med Särskilt yttrande (V)
- Remissvar från tekniska nämnden
- Fritidsnämnden beslut 220428 § 58
- Remissvar från fritidsnämnden
- Funktionsstödsnämnden beslut 220425 § 54
- Remissvar från funktionsstödsnämnden
- Förskolenämnden beslut 220427 § 68
- Remissvar från förskolenämnden
- Arbetsmarknads- och socialnämnden beslut 220426 § 147
- Remissvar från arbetsmarknads- och socialnämnden
- Valnämnden beslut 220329 § 22
- Remissvar från valnämnden
- Miljönämnden beslut 220517 § 101
- Remissvar från miljönämnden
- Revisorskollegiet beslut 220323 § 50

Datum
2022-05-24

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.
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 informationssäkerhet i Malmö stad. Förslaget har varit på remiss hos samtliga förvaltningar vilket föranlett vissa mindre ändringar och förtydliganden i riktlinjen.

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 ett riskbaserat och systematiskt informationssäkerhetsarbete med ökad tydlighet avseende ansvar och mandat.
- Ny styrning avseende uppföljning och aktivitetsplanering.

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

1. Kommunstyrelsen godkänner föreslaget styrdokument *Malmö stads riktlinjer för informationssäkerhet* att gälla från 1 november 2022.
2. Kommunstyrelsen upphäver styrdokumentet *Riktlinjer och anvisningar för informationssäkerhet i Malmö stad* från och med 31 oktober 2022.

Beslutsunderlag

- G-Tjänsteskrivelse KSAU 220530 Antagande av nya riktlinjer för informationssäkerhet i Malmö stad
- Remissvar från arbetsmarknads- och socialnämnden
- Arbetsmarknads- och socialnämnden beslut 220426 § 147
- Valnämnden beslut 220329 § 22
- Remissvar från valnämnden
- Grundskolenämnden beslut 220420 § 54
- Remissvar från grundskolenämnden
- Remissvar från tekniska nämnden
- Remissvar från förskolenämnden
- Remissvar från hälsa-, vård- och omsorgsnämnden
- Remissvar från kulturnämnden
- Kulturnämnden beslut 220420 § 44
- Remissvar från funktionsstödsnämnden
- Funktionsstödsnämnden beslut 220425 § 54
- Remissvar från servicenämnden
- Servicenämnden beslut 220426 § 46 med Särskilt yttrande (M+C)
- Överförmyndarnämnden beslut 220425 § 28
- Remissvar från överförmyndarnämnden
- Remissvar från gymnasie- och vuxenutbildningsnämnden
- Gymnasie- och vuxenutbildningsnämnden beslut 220429 § 61
- Remissvar från stadsbyggnadsnämnden
- Stadsbyggnadsnämnden beslut 220427 § 132
- Förskolenämnden beslut 220427 § 68
- Remissvar från fritidsnämnden
- Fritidsnämnden beslut 220428 § 58
- Hälsa-, vård- och omsorgsnämnden beslut 220429 § 62
- Tekniska nämnden beslut 220426 § 110 med Särskilt yttrande (V)
- Malmö stads riktlinjer för informationssäkerhet
- Remissvar från miljönämnden

Beslutsplanering

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

Beslutet skickas till

Samtliga nämnder

1.Ärendet

Nuvarande riktlinjer togs fram 2013 (se ärende STK-2013-224) och har sedan dess reviderats ungefär vartannat år för att passa verksamhetens utmaningar och 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 pandemin samt stadskontorets vilja att vänta in och beakta utfallet av de nya IT- och digitaliseringsriktlinjerna samt att den nya IT-organisationen skulle etablera sig hos serviceförvaltningen.

2.Sammanfattning av remissvaren
Yttranden har inkommit från samtliga remissinstanser med undantag för revisorskollegiet som avstår från att yttra sig över föreslagen riktlinje. Det sammantagna intrycket är att nämnderna är positiva till förslaget och att en ny riktlinje och dokumentstruktur är välkommen och välbehövd. Flera nämnder konstaterar att förslaget innebär en ambitionshöjning men framhäver samtidigt att nya riktlinjen kommer att underlätta fortlöpande översyn och bidra till högre efterlevnad och effektivitet inom området. Tydligheten avseende ansvar och mandat samt dokumentets fokus på riskbild och systematiskt arbetssätt lyfts fram av flera nämnder som en klar förbättring i jämförelse med nu gällande styrdokument. Även flytten av detaljkrav till underliggande anvisningar (som beslutas på tjänstepersonsnivå) lyfts fram som en mycket positiv förändring som förväntas medföra att kraven lättare kan hållas uppdaterade och kompletteras vid behov.

Utöver ovanstående har nämnderna även framfört olika synpunkter. Nedan följer en summering av återkommande synpunkter och förbättringsförslag:

1. Eftersom underliggande anvisningar inte är färdigställda föreslår 6 av 14 nämnder att befintligt styrdokument ska fortsätta gälla tills dess att underliggande anvisningar är klara. Detta är för att undvika ett ”gap” där Malmö stad står utan beslutade detaljkrav under en övergångsperiod tills de nya anvisningarna är framtagna och beslutade.

2. För att kunna rekrytera rätt person med rätt kompetens till samordnarrollen efterfrågar 5 av 14 nämnder att riktlinjen ska fördjupa sig kring samordnarens roll och uppdrag.

3. I och med Stadskontorets och Serviceförvaltningens betydande roller för informationssäkerhets- och IT-säkerhetsarbetet i staden så efterfrågar 5 av 14 nämnder att riktlinjen ska tydliggöra hur och vem som ska besluta om underliggande anvisningar och rutiner.

4. Behovet av utbildningsinsatser på både nämnds- och stadsövergripande nivå lyfts fram som avgörande för att öka medvetenheten hos ledning, chefer och medarbetare i organisationen. Därmed efterfrågar 7 av 14 nämnder ett förtydligande om stadskontorets roll i att både ta fram och erbjuda stadsövergripande utbildningar.

5. För att kunna efterleva föreslagen riktlinje efterfrågar 8 av 14 nämnder ett förtydligande i stadskontorets roll att erbjuda både verktyg och stöd i planerings-, genomförande- och uppföljningsarbetet inom ramen för riktlinjens omfattning.

6. Eftersom underliggande anvisningar saknas uppger 7 av 14 nämnder att det är svårt att resonera ifall föreslagen riktlinje kommer innebära några ökade kostnader.

3.Stadskontorets bedömning

I remissen efterfrågade stadskontoret i synnerhet synpunkter på nedanstående frågor. Här summeras de inkomna svaren och därefter följer stadskontorets ställningstagande med beaktande av inkomna remissvar.

3.1 Är riktlinjen tydlig avseende nämndens ansvar och uppdrag?

Samtliga nämnder utrycker att föreslagen riktlinje är mycket tydligare avseende nämndernas ansvar och uppdrag i jämförelse med nuvarande styrdokument. Flera nämnder lyfter att det är positivt att föreslagen riktlinje tydliggör att ansvaret för informationshantering och därmed även för informationssäkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen. Förskolenämnden föreslår en mindre korrigering i skrivningen av nämndens ansvar under punkt 2.3 i föreslagen riktlinje. Nämnden menar att föreslagen skrivning går att tolka som att nämndens ansvar enbart innebär att riktlinjen och underliggande styrdokument efterlevs.

Utifrån ovanstående bakgrund gör stadskontoret bedömningen att nämndernas ansvar är tydligt beskrivet, men har genomfört en mindre korrigering av lydelsen i punkt 2.3. Detta för att tydliggöra att nämndens ansvar sträcker sig bortom att endast tillse att riktlinjen och underliggande styrdokument efterlevs.

3.2 Är samordnarens roll, ansvar och uppdrag tillräckligt tydlig?

Samtliga nämnder utrycker att föreslagen riktlinje är mycket tydligare avseende informationssäkerhetssamordnaren roll och uppdrag. Flera nämnder efterfrågar dock en fördjupad uppdragsbeskrivning i riktlinjen. Dessutom framhävs behovet av bra underlag för kravprofil som kan användas vid rekrytering.
Utifrån ovanstående bakgrund gör stadskontoret bedömningen att samordnarens roll och uppdrag är tydliggjort i föreslagen riktlinje men behöver fördjupas ytterligare för att möta nämndernas behov. Stadskontoret gör dock bedömningen att rollen inte behöver fördjupas ytterligare i föreslagen riktlinje utan ska istället fördjupas i andra dokument. En fördjupad rollbeskrivning samt kravprofil har under våren 2022 tagits fram av stadskontoret och kommer finnas tillgänglig för stadens förvaltningar att använda som stödmaterial innan juli 2022.

3.3 I vilken omfattning kommer förslaget att påverka nämndens ansvarsområde?

En majoritet av nämnderna utrycker att nämndens ansvarsområde inte påverkas. Undantaget är servicenämnden som framhäver att föreslagen riktlinje får stor påverkan på nämndens uppdrag främst kopplat till det ansvar som förvaltningens IT- och digitaliseringsavdelning (hädanefter ITD) förfogar över. Nämnden lyfter behovet av att;

1. Servicenämndens ansvar definieras i riktlinjen
2. Hur föreslagen riktlinje förhåller sig till styrdokumentet *”Riktlinjer för IT- och digitalisering”*
3. Hur föreslagen riktlinje påverkar ITD mandat och styrning av stadens digitaliseringsarbete och kommungemensam IT.

Utifrån ovanstående bakgrund gör stadskontoret bedömningen att föreslagen riktlinje inte kommer påverka nämndernas ansvarsområden. Stadskontoret anser att den nya riktlinjen harmoniserar väl med innehållet i styrdokumentet *”Riktlinjer för IT- och digitalisering”* och inte innebär några motsättningar avseende servicenämndens eller IT- och digitaliseringsavdelningens roll och

ansvar för kommungemensam-IT och stadens digitaliseringsarbete.

För att så långt som möjligt tydliggöra servicenämndens respektive kommunstyrelsens olika ansvarsområden har följande korrigeringar vidtagits:

1. Ansvaret för att besluta om underliggande anvisningar är nu fastställt under punkten 2.4 i föreslagen riktlinje, där står följande; ”Stadsdirektören beslutar om stadsövergripande anvisningar för informationssäkerhet med rätt att vidaredelegera till;
   -Enhetschef-säkerhet och beredskapsenheten
   -Avdelningschef-IT och digitaliseringsavdelningen
   Vilket även framgår av kommunstyrelsens delegationsordning.”
2. Begreppet ”kommungemensam IT” har hämtats från styrdokumentet *”Riktlinjer för IT- och digitalisering”* och lagts till under rubriken definitioner i föreslagen riktlinje.
3. För att hänvisa till andra stadsövergripande styrdokument som påverkar Malmö stads arbete med informationssäkerhet har en ny rubrik lagts till i riktlinjens bilaga, se rubriken ”Referenser och definitioner”. Här hänvisas läsaren till bland annat till styrdokumentet *”Riktlinjer för IT- och digitalisering”*. Detta är enligt stadskontoret en mer ändamålsenlig lösning än att föreslagen riktlinje ska innehålla skrivningar som redan finns beslutande i till exempel styrdokumentet *”Riktlinjer för IT- och digitalisering”*.

3.4 Vilket stöd behöver nämnden från kommunstyrelsen för att implementera riktlinjerna?

Samtliga nämnder uttrycker behov av någon form av stöd eller vägledning från stadskontoret. Främst handlar det om stadsövergripande utbildningspaket för att öka medvetenheten hos medarbetarna men även fler rutiner och verktyg för planering, genomförande och uppföljning. Nämnderna efterlyser även stadskontorets ledning i utformandet av stadsövergripande informationssäkerhetsmål samt uppdaterade metoder för riskanalys, informationsklassificering och incidentrapportering

Utifrån ovanstående bakgrund gör stadskontoret bedömningen att nämnderna måste få mer stöd och vägledning för att implementera föreslagen riktlinje. Vidare bedöms nämndernas önskemål vara helt i linje med stadskontorets åtagande och ansvar. Stadskontoret kommer leverera anvisningar, rutiner och underlag för att stadens nämnder ska kunna implementera, efterleva och följa upp riktlinjen på ett ändamålsenligt sätt.

3.5 Innebär förslaget några ekonomiska konsekvenser för nämnden? I så fall i vilken omfattning?

En majoritet av nämnderna uttrycker att det är svårt att ta ställning till eventuella ekonomiska konsekvenser utan att underliggande anvisningar finns på plats. Ett fåtal nämnder lyfter fram att rekrytering av informationssäkerhetssamordnare kommer innebära ökade kostnader.

Utifrån ovanstående bakgrund föreslår stadskontoret att kommunstyrelsen delar detta synsätt och vill framhäva att den ekonomiska aspekten är viktig att ha med sig i det fortsatta arbetet vid framtagning av nya stadsövergripande anvisningar och rutiner som kan komma att vara kostnadsdrivande för nämnderna att implementera och efterleva.

Ansvariga

Per-Erik Ebbeståhl Avdelningschef
Magdalena Bondeson Sektionschef
Andreas Norbrant Stadsdirektör

Malmö stad

2022-06-20

Dokumentets namn:
Malmö stads riktlinjer för informationssäkerhet

Diarienummer:
STK-2021-1717

Typ av dokument:
Riktlinje

Version:
1.0

Beslutad av:
Kommunstyrelsen

Datum för beslut:
2022-06-07

Framtagen av:
Stadskontoret

Organisation/område:
Samtliga nämnder

Ansvarig chef:
Ulf Nilsson

Uppföljd:

Reviderad av:

Reviderad:

Malmö stads riktlinjer för informationssäkerhet

Innehåll

1. Inledning

1.1 Bakgrund

Stora mängder information skapas och behandlas dagligen av Malmö stads medarbetare och verksamheter. Informationen finns överallt, till exempel på papper, datorer, på whiteboard- och anslagstavlor, molntjänster, verksamhetssystem och i arkiven. Bristande informationssäkerhet innebär alltid sårbarheter och inte sällan även lagbrott i vår informationshantering. 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.

En av informationssäkerhetens största utmaningar är att informationen alltid ska ha ett tillräckligt skydd, utan att verksamheter och medarbetare upplever att implementerade säkerhetsåtgärder hindrar dem från att utföra sitt uppdrag. Genom att säkerställa att informationssäkerhet finns med som ett perspektiv i alla delar av stadens verksamheter och uppdrag kan vi tillsammans arbeta för att skydda informationen på ett tillräckligt och avvägt sätt.

1.2 Syfte och omfattning

Syftet med denna riktlinje är att på strategisk nivå fastställa ansvar, målsättning och arbetssätt för informationssäkerhet i Malmö stad och därigenom sätta ramarna för hur allt arbete med informationssäkerhet ska bedrivas. Detaljerade krav, beskrivningar och vägledning som förklarar hur stadens verksamheter ska implementera innehållet i denna riktlinje kommer att finnas i underliggande anvisningar, regler och rutiner.

Riktlinjen gäller för all hantering och alla typer av Malmö stads information. Oavsett om den är fysisk eller digital och oberoende av i vilken form eller sammanhang informationen förekommer. Därmed ska denna riktlinje och underliggande styrdokument alltid beaktas vid framtagning och revidering av andra styrdokument som påverkar Malmö stads informationshantering. Innehållet i riktlinjen och underliggande anvisningar, regler och rutiner baseras på standarden för informationssäkerhet SS-ISO/IEC 27000-serien. Dessa dokument bildar tillsammans stadens ledningssystem för informationssäkerhet (LIS).

1.3 Revidering och uppföljning

Riktlinjen revideras vid behov och gäller för stadens nämnder. Efterlevnaden av riktlinjen följs upp löpande och sammanställs av stadskontoret i en årlig återkoppling till stadens ledningsgrupp och kommunstyrelsen.

2. Ansvar

2.1 Ansvarsprincipen

Ansvaret för informationshantering och därmed även för informations-säkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen. Detta ansvar gäller från nämnd till enskild medarbetare. Utöver detta gäller att den som är ansvarig ensamt eller tillsammans med andra för en viss process, projekt eller uppdrag även ansvarig för informationssäkerheten inom sitt ansvarsområde.

2.2 Kommunstyrelsen

Kommunstyrelsen har enligt sitt reglemente det övergripande ansvaret för stadens informationssäkerhet och beslutar om riktlinjer för informationssäkerhet.

2.3 Nämnd

Varje nämnd är ansvarig för informationssäkerheten inom sin förvaltning. Nämnden ska tillse att denna riktlinje och underliggande styrdokument efterlevs.

2.4 Stadsdirektören

Stadsdirektören beslutar om stadsövergripande anvisningar för informationssäkerhet med rätt att vidaredelegera till;
-Enhetschef-Säkerhet och beredskapsenheten
-Avdelningschef-IT och digitaliseringsavdelningen
Allt i enlighet med kommunstyrelsens delegationsordning.

2.5 Verksamhetsansvarig

Chef (oavsett nivå) ansvarar för informationssäkerheten inom sin verksamhet. Varje chef ansvarar för att deras medarbetare efterlever riktlinjen, har ett riskbaserat arbetssätt samt tillräcklig förståelse och kunskap för att nödvändig informationssäkerhet i verksamheten uppnås. Det inkluderar information och utbildning till medarbetare samt ekonomiskt och säkerhetsmässigt ansvar.

2.6 Medarbetare

Alla medarbetare har ett eget ansvar för verksamhetens informationssäkerhet och ska i sitt eget arbete efterleva gällande styrdokument. Varje anställd har en skyldighet att rapportera informationsrelaterade brister och incidenter.

3. Målsättning

3.1 Målområden

Nedanstående målområden beskriver vad Malmö stad ska uppnå med sitt informationssäkerhetsarbete och ska alltid beaktas vid val av insatser för att höja informationssäkerheten. Respektive målområde fördjupas i efterföljande kapitel med samma namn.

3.2 Informationshantering

Ansvaret för informationssäkerheten ska vara tydligt. All information som Malmö stad äger eller på annat sätt ansvarar för ska behandlas på ett säkert och korrekt sätt. Skyddet av information ska anpassas efter dess skyddsvärde, rådande förutsättningar, hot och risker.

3.3 Medarbetare

Alla medarbetare ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sin roll och arbetsuppgifter. De ska vara säkerhetsmedvetna och ha god kännedom om de hot och risker som finns och hur de kan skydda sig mot dem. Det gäller även konsulter, leverantörer, praktikanter och personuppgiftsbiträden samt andra uppdragstagare som behandlar information för Malmö stads räkning.

3.4 Process

Informationssäkerhet ska vara ett integrerat perspektiv och en medveten del av verksamhetens arbetsprocesser och informationshantering. Arbetet ska bedrivas genom ett systematiskt, riskbaserat och långsiktigt perspektiv samt involvera relevanta kompetenser utifrån informationens skyddsvärde och verksamhetens behov.

3.5 Teknik

Malmö stads informationssystem ska vara robusta, funktionella och säkra med utgångspunkt i informationens skyddsvärde, riskbild och verksamhetens behov. Detta inkluderar även de informationssystem som Malmö stad köper in.

4. Informationshantering

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen och i enlighet med nämndernas reglementen. Med information menas all information oavsett i vilken form eller sammanhang den förekommer, analog som digital. Informationens skyddsvärde beror på dess innehåll, sammanhang och syftet med dess behandling. Skyddsvärdet styr hur informationen ska behandlas. Att informationen ska behandlas utifrån rådande förutsättningar, hot och risker betyder att lagar, förordningar, interna policys, riktlinjer, anvisningar och aktuell riskbild alltid ska sammanvägas för att ge informationen ett korrekt skyddsvärde.

- För att identifiera informationens skyddsvärde ska den klassificeras och dess hantering riskbedömas.
- Information ska utifrån sitt skyddsvärde och riskbild skyddas med lämpliga organisatoriska, administrativa, fysiska och tekniska säkerhetsåtgärder utifrån perspektiven konfidentialitet, riktighet och tillgänglighet.
- Informationssäkerheten ska hålla samma nivå oberoende i vilken form och sammanhang som informationen behandlas.
- Information ska som regel endast vara tillgänglig för de personer som behöver informationen inom sitt uppdrag i syfte att kunna utföra sin arbetsuppgift.
- Vid prioritering av informationssäkerhetsåtgärder ska de informationsmängder som har högst skyddsvärde och riskbild åtgärdas först.

5. Medarbetare

Information och utbildning inom informationssäkerhet ska vara en del av anställningsprocessen likväl vid anställningens upphörande. Information och utbildning ska stå i proportion till den anställdes roll och uppdrag samt de hot och risker som kan förekomma i den anställdes informationshantering.

- Alla anställda ska erbjudas information och utbildning i informationssäkerhet. Kunskapen ska hållas aktuell och kompletteras utefter behov och inom ramen för sitt uppdrag.
- Konsulter och övriga uppdragstagare som behandlar information för Malmö stads räkning ska få anpassad information och utbildning i informationssäkerhet utifrån sitt uppdrag.
- Anställda ska vara observanta och hålla sig informerade om informationssäkerhetshot och risker samt rapportera risker och incidenter.

6. Process

6.1 Integrerat perspektiv

Riktlinjen ska tillsammans med underliggande styrdokument arbetas in i befintliga verksamhetsprocesser och rutiner av de som är ansvariga för dem. I de fall verksamhetsspecifika rutiner saknas är det upp till respektive verksamhet att utifrån identifierat behov ta fram kompletterande rutiner.

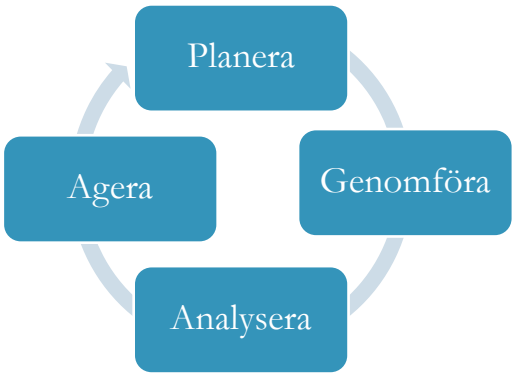
Det ska finnas möjlighet för varje förvaltning att besluta om tidsbegränsade avsteg från underliggande anvisningar. I sådana fall ska det finnas ett beslutsunderlag bestående av dokumenterad riskanalys och motivering till beslut.

6.2 Systematiskt arbetssätt

För att åstadkomma ett systematiskt, riskbaserat och långsiktigt informations-säkerhetsarbete samtidigt som kvalitén i arbetet upprätthålls ska allt arbete inom området bedrivas på följande sätt:

- **Planera:** Utifrån lagstiftning, styrdokument, informationsklassificeringar, incidenter och riskbedömningar identifiera och planera att införa säkerhetshöjande åtgärder.
- **Genomföra:** Genomföra planerade åtgärder.

- **Analysera:** Utvärdera införandet. Kontrollera att syftet med åtgärderna är uppfyllt.
- **Agera:** Ta fram förslag på nya säkerhetshöjande åtgärder.



6.3 Kommunstyrelsen

Kommunstyrelsen har i enlighet med sitt reglemente ansvar för det övergripande arbetet med informationssäkerhet och ska leda, samordna och ha uppsikt över området. Detta innebär att utifrån ett helhetsperspektiv leda och samordna stadens övergripande arbete, ta fram stadsövergripande styrdokument och processer samt följa upp att de efterlevs. Stadskontoret har därmed som styrelsens förvaltning ett centralt, stadsövergripande ansvar att sätta ramarna för hur allt arbete med informationssäkerhet i Malmö stad ska bedrivas. I detta ansvar ingår;

- Förvalta och utveckla riktlinjen för informationssäkerhet
- Förvalta och utveckla stadsövergripande processer, regler och rutiner för informationsklassificering, riskanalys, avsteg, incidenthantering och uppföljning.
- Förvalta och utveckla systemstöd för klassificering och kravställning av Malmö stads information och informationssystem.
- Leda, utveckla och stödja stadens informationssäkerhetsnätverk.
- Utbilda och vägleda verksamheter i både stadsövergripande och verksamhetsspecifika informationssäkerhetsfrågor.
- Följa upp stadens arbete med informationssäkerhet och rapportera resultatet till stadens ledningsgrupp och kommunstyrelsen.

6.4 Nämnder

Varje nämnd är ansvarig för informationssäkerheten inom sin förvaltning. Nämnden ska tillse att denna riktlinje och underliggande styrdokument efterlevs. Varje förvaltning ska bedriva ett systematiskt, riskbaserat och långsiktigt informationssäkerhetsarbete. Efterlevnaden ska årligen följas upp och rapporteras till den egna förvaltningsledningen och nämnden.

Varje förvaltningsledning ska utse en informationssäkerhetssamordnare som ansvarar för att samordna och följa upp förvaltningens interna informationssäkerhetsarbete. Rollen ska arbeta långsiktigt och verksamhetsövergripande för att informationssäkerhet ska integreras i förvaltningens verksamheter av de som är ansvariga för dem. Samordnaren är stadskontorets motpart inom området och kommer att inkluderas i kommunens övergripande strategiska arbete. För att uppnå en god förmåga i staden ska samordnaren ges utrymme att arbeta strategiskt och tillsammans med motsvarande roller i andra förvaltningar. Inom uppdraget ska det finnas tid för innovation, omvärldsbevakning och kunskapsutveckling. Rollen ansvarar även för att:

- Rapportera till förvaltningsledningen.
- Vara förvaltningens representant i Malmö stads interna informationssäkerhetssamordnarnätverk.
- Kunna leda och bistå med kompetens vid genomförande av informationsklassificeringar.
- Kunna leda och bistå med kompetens vid riskanalyser inom ramen för riktlinjens omfattning.

7. Teknik

Informationssäkerhetsperspektivet ska alltid beaktas vid all IT-användning under hela dess livscykel, från behov till avveckling. Identifiering av informationssäkerhetskrav ska integreras tidigt i samtliga IT-processers livscykel och finnas med kontinuerligt under alla delar av förändringshantering.

- All IT, inklusive kommungemensam-IT, digital infrastruktur, informationssystem och digitala tjänster ska ha en utpekad och dokumenterad ägare som är ansvarig för att säkerställa skyddet av informationen.
- Det ska finnas en stadsövergripande förvaltningsmodell för Malmö stads informationssystem.

Bilaga. Referenser och definitioner

Referenser

Nedanstående styrdokument har betydelse för stadens informationshantering och ska därmed också tas i beaktning vid arbetet med informationssäkerhet;

1.Trygghets- och säkerhetspolicy för Malmö stad, antagen av KF 2017-05-24

2.Riktlinjer för behandling av personuppgifter i Malmö stad, antagen av KS 2018-05-02

3.Arkivhandbok för Malmö stad, KSAU 2018-08-27

4.Programmet för Malmö stads digitalisering 2017 – 2022, antagen av KF 2017-03-01

5.Riktlinjer för IT och digitalisering, antagen av KF 2021-03-31

Definitioner

Behandling/Hantering: En åtgärd eller kombination av åtgärder beträffande information, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. (MSBFS:2020:6)

Incident: En oförutsedd händelse som får en oönskad effekt i form av skada för individ eller verksamhet.

Information: All information oavsett form eller sammanhang. (MSB-Publikationsnummer MSB976)

Informationsklassificering: Arbetsmetod för att säkerställa att information får en lämplig säkerhet med hänsyn till informationens skyddsvärde och riskbild. Informationens skyddsnivå säkerställs med lämpliga organisatoriska, administrativa, fysiska och tekniska säkerhetsåtgärder utifrån perspektiven konfidentialitet, riktighet och tillgänglighet. (MSB-Publikationsnummer MSB976)

Informationssystem: Samlingsnamn för alla typer av IT-system och digitala tjänster och applikationer som hanterar information. I begreppet ingår också nätverk och digital infrastruktur. (MSBFS:2020:6)

Informationssäkerhet: Bevarandet av konfidentialitet, riktighet och tillgänglighet hos information. (MSBFS:2020:6)

Informationsägare: Person som ansvarar för att informationen skyddas på avsett sätt. (MSBFS:2020:6)

Risk: Sannolikheten för att en oönskad händelse inträffar och konsekvenserna som detta i så fall skulle innebära. (MSB-Publikationsnummer MSB976)

Konfidentialitet: Att information endast är tillgänglig för de som har behörighet att ta del av informationen.

Kommungemensam IT: Omfattar den kommungemensamma digitala infrastrukturen, IT-plattformar samt processer och kompetenser som används av alla eller några förvaltningar.

Ledningssystem för informationssäkerhet (LIS): Del av myndighetens övergripande ledningssystem. Syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhetsarbete. (MSBFS:2020:6)

Riktighet: Att information är korrekt, aktuell och fullständig samt att den inte förändras, varken av obehörig eller av misstag.

Riskanalys: Strukturerat arbetssätt för att identifiera, bedöma och hantera hot, risker och sårbarheter.

Skyddsvärde: Informationens säkerhets- och hanteringsbehov utifrån bedömning av konfidentialitet, riktighet och tillgänglighet, gällande lagar och aktuell riskbild.

Tillgänglighet: Åtkomst till information för behörig person vid rätt tillfälle. (Terminologi informationssäkerhet, SIS-TR 50:2015)