Trafikförvaltningen
Förvaltning för utbyggd tunnelbana

TJÄNSTEUTLÅTANDE
2020-10-14

Trafiknämnden
2020-11-24, punkt 7

Ärende
TN 2020-0446

Infosäkerhetsklass
K1 (Öppen)

Yttrande över förslag till ny policy för verksamhetsskydd Region Stockholm”

Ärendebeskrivning

Rotel I har remitterat för yttrande förslag till ny policy för verksamhetsskydd inom Region Stockholm att ersätta nuvarande informationssäkerhetspolicy samt säkerhetspolicy. I ärendet återkommer nämnden med yttrande över förslaget.

Beslutsunderlag

Förvaltningschefernas tjänsteutlåtande 2020-10-14 inklusive bilaga 1 med yttrande över förslag till ny policy för verksamhetsskydd inom Region Stockholm
Remiss, RS 2020-0147, inklusive

1. Remiss-PM: Policy för verksamhetsskydd
2. Remiss: Policy Verksamhetsskydd

Förslag till beslut

Förvaltningscheferna för trafikförvaltningen och förvaltningen för utbyggd tunnelbana föreslår att trafiknämnden beslutar följande.

1. Trafiknämnden avger yttrande enligt bilaga 1.

2. Paragrafen justeras omedelbart.

Trafikförvaltningen
Förvaltning för utbyggd tunnelbana

TJÄNSTEUTLÅTANDE
2020-10-14

Ärende
TN 2020-0446

Infosäkerhetsklass
K1 (Öppen)

Förslag och motivering

I enlighet med Region Stockholms ambition att konsolidera de styrande dokumenten i syfte att minska den administrativa överbyggnaden och detaljstyrningen föreslås en ny policy för verksamhetsskydd ersätta nuvarande informationssäkerhetspolicy och säkerhetspolicy inom Region Stockholm. Den nya policyn föreslås även vara utgångspunkten för allt arbete med kontinuitet och krisberedskap.

Den nya policyn är utformad så att den till utformning och innehåll kompletterar beslutad ambition inom området samt inriktning för integrerad ledning och styrning enligt Region Stockholm budget 2020. Följaktligen innehåller policyn inga mål utan definierar istället syfte och omfattning för verksamhetsskyddet. Vidare definieras den gemensamma utgångspunkten och de styrande principer som ska gälla för samtliga nämnders och bolags arbete för att skydda verksamheten. Skrivningar som anger principer och krav på en mer detaljerad nivå har tagits bort för att istället hanteras i underliggande riktlinjer och strategier. Skrivningar avseende ansvar som redan anges i Region Stockholm budget tas bort då de utgör upprepningar. Enbart tillkommande ansvar och roll som är nödvändig för ett systematiskt arbete med verksamhetsskydd är medtagen.
Allt arbete med skyddsåtgärder inom fysisk säkerhet, personalsäkerhet, informationssäkerhet, kontinuitet och krisberedskap föreslås utgå från den nya policyn för verksamhetsskydd. Under året kommer kompletterande riktlinjer och vägledningar successivt tas fram. Den nya policyn har även givits en förenklad struktur i syfte att underlätta för chefer och medarbetare i Region Stockholm att förstå och följa den.

Trafiknämnden är överlag positiv till den nya policyn och dess inriktning. Nämndes yttrande återfinns i bilaga 1.

Ekonomiska konsekvenser
Beslut om policyn i sig innebär inga direkta kostnader. Realisering av ambitionerna inom området informationssäkerhet kräver dock ekonomiska insatser, som ska beaktas i ordinarie verksamhetsplanering och budgetarbete. Ett adekvat utformat verksamhetsskydd bör bidra till minskade ekonomiska konsekvenser i form av förluster av olika slag och minskad risknivå. Hur stora kostnaderna blir beror på vilken ambitionsnivå respektive verksamhet och Region Stockholm som helhet sätter för sitt informationssäkerhetsarbete.

Riskbedömning
Förslaget bedöms inte medföra några nya risker utan snarare förbättra dagens riskbild.

Konsekvenser för miljön
Förslaget bedöms inte medföra några negativa konsekvenser för miljön.

Sociala konsekvenser
Förslaget bedöms ha positiva sociala konsekvenser genom ökat fokus på säkerhet, skydd och trygghet.

Niklas Bergman
Förvaltningschef
Förvaltning för utbyggd tunnelbana

David Lagneholm
Förvaltningschef
Trafikförvaltningen

Trafikförvaltningen
Förvaltning för utbyggd tunnelbana

TJÄNSTEUTLÅTANDE
2020-10-14

Ärende
TN 2020-0446

Infosäkerhetsklass
K1 (Öppen)

Bilaga 1

Yttrande

Bakgrund
I enlighet med Region Stockholms ambition att konsolidera de styrande dokumenten i syfte att minska den administrativa överbyggnaden och detaljstyrningen föreslås en ny policy för verksamhetsskydd ersätta nuvarande informationssäkerhetspolicy och säkerhetspolicy inom Region Stockholm. Den nya policyn föreslås även vara utgångspunkten för allt arbete med kontinuitet och krisberedskap.

Den nya policyn är utformad så att den till utformning och innehåll kompletterar beslutad ambition inom området samt inriktning för integrerad ledning och styrning enligt Region Stockholm budget 2020. Följaktligen innehåller policyn inga mål utan definierar istället syfte och omfattning för verksamhetsskyddet. Vidare definieras den gemensamma utgångspunkten och de styrande principer som ska gälla för samtliga nämnders och bolags arbete för att skydda verksamheten. Skrivningar som anger principer och krav på en mer detaljerad nivå har tagits bort för att istället hanteras i underliggande riktlinjer och strategier. Skrivningar avseende ansvar som redan anges i Region Stockholm budget tas bort då de utgör upprepningar. Enbart tillkommande ansvar och roll som är nödvändig för ett systematiskt arbete med verksamhetsskydd är medtagen.
Allt arbete med skyddsåtgärder inom fysisk säkerhet, personalsäkerhet, informationssäkerhet, kontinuitet och krisberedskap föreslås utgå från den nya policyn för verksamhetsskydd. Under året kommer kompletterande riktlinjer och vägledningar successivt tas fram. Den nya policyn har även givits en förenklad struktur i syfte att underlätta för chefer och medarbetare i Region Stockholm att förstå och följa den.

Trafiknämnden har ombetts yttra sig över förslaget till ny policy.

Övergripande synpunkter

Trafiknämnden har tagit del av den promemoria som åtföljs förslaget till policy för verksamhetsskydd Region Stockholm och har följande medskick till den bakgrund och inriktning som ges i promemorian

- Att minska den administrativa överbyggnaden är positivt. En verksamhetsskyddspolicy bör bygga på lagar, nationella säkerhetsstrategin och en riskbild/RSA (KRSA) som ska mynna ut till olika områden som policyn bör omfatta:
    - Säkerhetsskydd (informationssäkerhet, fysisk säkerhet, personalsäkerhet)
    - Signalskydd
    - Informationssäkerhet
    - Brandsäkerhet
    - Fysisk säkerhet
    - Trafiksäkerhet
    - IT-säkerhet
    - Oegentligheter (muta, jäv m.m.)
    - Flygplatssäkerhet
    - Personsäkerhet (hot, våld och otillåten påverkan, skyddad identitet, resor m.m.)
    - Civilförsvarsplanering
    - Krisberedskap och kontinuitetsplanering

- Nämnden är positiv till att man inte upprepar samma sak i flera dokument. Dock försvårar det möjligheten att på ett enkelt sätt få en helhetsbild av vad som avses med verksamhetsskydd.

Policy för verksamhetsskydd

Sida 2: 1.3, första stycket

- Allt arbete utgår från lagstiftning och Sveriges nationella säkerhetsstrategi, föreliggande policy ska sedan förtydliga regionens egen ambition.
- Samordnare används normalt i arbete med informationssäkerhet. Var och hur många samordnare finns det och är de centralt placerade? Att ha samordnare innebär en kostnad för verksamhetsskyddet. Förvaltningar och bolag är organiserade med säkerhetschef. Begreppet samordnare kan läsas som en roll utan faktisk ansvar och mandat, en enbart samordnande funktion, således ingen bra benämning.
- *inom området*: vilket område är det som avses? Meningen avslutas med ordet *verksamhetsskyddet*, avser ordet *området* detta ord?

Sida 2: 1.3, andra stycket

- Att minska den administrativa överbyggnaden är positivt. En verksamhetsskyddspolicy bör bygga på lagar, nationella säkerhetsstrategin och en riskbild/RSA (KRSA) som ska mynna ut till olika områden som policyn bör omfatta:
    - Säkerhetsskydd (informationssäkerhet, fysisk säkerhet, personalsäkerhet)
    - Signalskydd

- Informationssäkerhet
- Brandsäkerhet
- Fysisk säkerhet
- Trafiksäkerhet
- IT-säkerhet
- Oegentligheter, otillbörlig påverkan
- Flygplatssäkerhet
- Personsäkerhet (hot, våld och otillåten påverkan, skyddad identitet, resor m.m.)
- Civilförsvarsplanering
- Krisberedskap och kontinuitetsplanering

Sida 2: 2, först stycket, punkt 1, förslag till ändring

- *Invånare och besökare: Alla som nyttjar Region Stockholms tjänster ska vara säkra och känna sig trygga när de tar del av Region Stockholms verksamheter.*

Sida 3: 2, första stycket, punkt 1

- För att undvika eventuella missförstånd bör en ny sista mening läggas till, *Ansvaret för arbetsmiljön åvilar respektive arbetsgivare.*

Sida 3: 2, andra stycket, rubriken

- Ordet *ändamålsenligt* bör läggas till före ordet *dimensionerat*.

Sida 3: 2, andra stycket, punkt 1

- Ordet *risktolerans* är inte vedertaget inom säkerhet och trygghet, utan används företrädesvis inom det ekonomiska området. Om det endast är den ekonomiska toleransen som avses är ordvalet lämpligt.
- Förenkla meningen genom att avsluta med *oacceptabel påverkan på verksamheten.*

Sida 3: 2, punkt 2

Förslag till ändring, nuvarande meningsuppbyggnad kan leda till feltolkning av text.

- Regions funktionalitet:
  - Arbetsprocesser och egendom såsom lokaler, infrastruktur, utrustning och information ska värderas och skyddas.
  - Region Stockholm ska ha förmåga att förebygga störningar och kriser och minska konsekvenserna om de ändå inträffar.
  - Länets invånare och andra aktörer ska känna tillit att Region Stockholm har denna förmåga.

Sida 3: 2, andra stycket, punkt 2

- Förslag till ny formulering: *Skyddet ska vara dimensionerat utifrån vid var tid aktuell hot- och riskbild och anpassas till lagkrav och skyddsvärde.*

Sida 3: 2, andra stycket, punkt 2

- Förslag till ny formulering: *Arbetet ska bedrivas systematiskt och spårbart, med ständiga förbättringar som en integrerad del i Region Stockholms övriga verksamhetsplanering*.

Sida 3: 2, andra stycket, punkt 5

- Förenkla meningen genom att avsluta med *oacceptabel påverkan på verksamheten*.

Sida 3: 2, andra stycket

- Förslag till ytterligare en punkt: *Region Stockholm ska verka för intern och extern samverkan i det förebyggande arbetet*.

Sida 3: 2, tredje stycket, rubriken

- För att tydliggöra innehållet i stycket föreslås att rubriken byts ut och ersätts med ordet: *Effektmål*. Om så inte sker, stavfel, Skyddsåtgärder

Sida 3: 2, tredje stycket, underrubriken

- Ordet S*kyddsåtgärderna* används endast en gång i dokumentet. Förslag att ändra till ordet *Verksamhetsskyddet*.

Sida 3: 2, tredje stycket, punkt 1

- Förslag att stryka orden: *där skyddsvärd verksamhet bedrivs*. Obehöriga ska inte ha tillträde någon del av regionens verksamheter.

Sida 3: 2, tredje stycket, punkt 2

- Förslag att lägga till ordet *skyddsvärda* före ordet *informationstillgångar*.

Region Stockholm

Regionledningskontoret

PM
2020-03-24

RS 2020-0147

Verksamhetsskyddspolicy

Remiss-PM

Innehållsförteckning

1. Regionledningskontorets förslag och motivering 3
1.1 Sammanfattning 3
1.2 Bakgrund 3

2. Sammanfattning av förändringar 3
2.1 Arbetsprocess och förankring 4
2.2 Ekonomiska konsekvenser 4

1. Regionledningskontorets förslag och motivering

1.1 Sammanfattning

I remissen föreslås en ny policy för verksamhetsskydd att ersätta nuvarande informationssäkerhetspolicy och säkerhetspolicy inom Region Stockholm. Den nya policyn föreslås även vara utgångspunkten för allt arbete med kontinuitet och krisberedskap. Remissen är ett led i beredningen av ärendet om verksamhetsskyddspolicy för Region Stockholm, avsett att beslutas om i regionfullmäktige den 17–18 november 2020.

1.2 Bakgrund

Region Stockholms främsta styrande dokument är budget. I denna anges ambitionen att de styrande dokumenten inom Region Stockholm ska konsolideras och bli färre. Syftet är att minska administrativ överbyggnad och detaljstyrning i möjligaste mån, och samtidigt säkra en styrning som håller samman.

2. Sammanfattning av förändringar

Nuvarande policys inom området verksamhetsskydd är:

- *LS 1112-1733 Informationssäkerhetspolicy* samt
- *LS 2015-0093 Policy för säkerhet*.

Dessa föreslås upphöra och ersättas med en gemensam policy för verksamhetsskydd i enlighet med denna remiss.

Policyn är utformade så att den till utformning och innehåll kompletterar beslutad ambition inom området samt inriktning för integrerad ledning och styrning enligt Region Stockholm budget 2020.

Följaktligen innehåller policyn inga mål utan definierar istället syfte och omfattning för verksamhetsskyddet. Vidare definieras den gemensamma utgångspunkten och de styrande principer som ska gälla för samtliga nämnders och bolags arbete för att skydda verksamheten. Skrivningar som anger principer och krav på en mer detaljerad nivå har tagits bort för att istället hanteras i underliggande riktlinjer och strategier.

Skrivningar avseende ansvar som redan anges i Region Stockholm budget tas bort då de utgör upprepningar. Enbart tillkommande ansvar och roll som är nödvändig för ett systematiskt arbete med verksamhetsskydd är medtagen.

Allt arbete med skyddsåtgärder inom fysisk säkerhet, personalsäkerhet, informationssäkerhet, kontinuitet och krisberedskap föreslås utgå från den nya policyn för verksamhetsskydd. Under året kommer kompletterande riktlinjer och vägledningar successivt tas fram.

I enlighet med Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården har skrivningar tagits med som möter föreskrifternas krav gällande informationssäkerhetspolicy.

Slutligen har den nya policyn givits en förenklad struktur i syfte att underlätta för chefer och medarbetare i Region Stockholm att förstå och följa den.

2.1 Arbetsprocess och förankring

Arbetet med förslaget till verksamhetsskyddspolicy har utgått från tidigare utredning och samråd inom området. I detta arbete deltog Regionledningskontoret, Hälso- och sjukvårdsförvaltningen och Trafikförvaltningen. Samråd har skett med Säkerhet och beredskap, Ekonomi och finans samt regelefterlevnad inom Regionledningskontoret.

2.2 Ekonomiska konsekvenser

Beslut om policyn i sig innebär inga direkta kostnader. Realisering av ambitionerna inom området informationssäkerhet kräver dock ekonomiska insatser, som ska beaktas i ordinarie verksamhetsplanering och budgetarbete. Hur stora kostnaderna blir beror på vilken ambitionsnivå respektive verksamhet och Region Stockholm som helhet sätter för sitt informationssäkerhetsarbete.

Grundprincipen är att varje nämnd och bolag ansvarar för de åtagande som verksamhetsskyddspolicyn vägleder inom och att respektive verksamhet identifierar de behov som finns och vilka åtgärder som behöver vidtas för detta. Med det följer även ansvar för finansiering av de egna insatserna. Informationssäkerhet ska beaktas vid beslut, verksamhetsplanering och budgetarbete på alla nivåer.

Region Stockholm

Diarienummer
RS 2020-0147

Remiss - Policy

Verksamhetsskydd

Gäller för Region Stockholm

Dokumenttyp	Fastställd	Giltig till och med
Dokumentnummer	Fastställd av	Upprättad av
Informationssäkerhetsklass		

1. Verksamhetsskyddspolicy

1.1 Inledning

Region Stockholm har ett viktigt samhällsuppdrag och ansvarar för hälso- och sjukvård, kollektivtrafik och regional utveckling i Stockholms län. Regionen bidrar även till kulturen i länet. Stora delar av Region Stockholms verksamhet är dessutom samhällsviktig. Region Stockholms verksamheter måste fungera såväl till vardags som vid oönskade händelser. Därför ska verksamheterna och de tillgångar som hanteras i dem skyddas mot hot och risker. Verksamheterna ska bedrivas med så få störningar och kriser som möjligt, och i de fall de uppkommer ska de kunna hanteras.

1.2 Syfte

Syftet med denna policy är att beskriva hur Region Stockholm ska arbeta, både regionövergripande och i nämnder och bolag var för sig, för att åstadkomma ett robust skydd av verksamheten i enlighet med regionfullmäktiges vision och inriktningsmål. Därigenom bidrar Region Stockholm till att skydda även samhällets skyddsvärden.

1.3 Tillämpning

Denna policy gäller för Region Stockholms nämnder och bolag. Den ska tillämpas i Region Stockholms verksamhetsplanering och i avtal med alla som arbetar på uppdrag av Region Stockholm. Allt arbete med verksamhetsskydd inom Region Stockholm utgår från denna policy. Ansvaret för skyddet av verksamheten är kopplat till det delegerade verksamhetsansvaret. Samordnare med stödjande funktion inom området ska stötta nämnder och bolag att aktivt driva på utvecklingen av verksamhetsskyddet.

Verksamhetsskyddspolicyn konkretiseras i tillhörande riktlinjer för säkerhet, informationssäkerhet och krisberedskapsplan, och kompletteras av Region Stockholms övriga styrande dokument.

2. Styrande principer

Region Stockholms arbete med verksamhetsskydd ska utgå från följande principer:

Region Stockholms verksamheter och tillgångar ska skyddas

Region Stockholms arbete med verksamhetskydd ska bedrivas för att värna om:

- Invånare och besökare: Alla som nyttjar Region Stockholms tjänster ska vara säkra och känna sig trygga när de tar del av Region Stockholms

verksamheter och vara förvissade om att information hanteras på ett säkert sätt.
- Medarbetare och förtroendevalda: Alla som arbetar inom eller har ett uppdrag för Region Stockholm ska vara säkra och känna trygghet när de utför sina uppgifter.
- Regionens funktionalitet: Arbetsprocesser och egendom såsom lokaler, infrastruktur, utrustning och information ska värderas och skyddas. Region Stockholm ska ha förmåga att förebygga störningar och kriser och minska konsekvenserna om de ändå inträffar. Länets invånare och andra aktörer ska känna tillit att Region Stockholm har denna förmåga.

Verksamhetskyddet ska vara dimensionerat
Det innebär att nämnder och bolag ska utgå från följande i sitt arbete med verksamhetsskydd:
- Verksamhetens risktagande ska återspegla nämnders och styrelsers risktolerans för att undvika oacceptabla skador, förluster och negativ verksamhetspåverkan.
- Skyddet ska dimensioneras utifrån aktuell hotbild och anpassas till skyddsvärde, risk och lagkrav.
- Arbetet ska bedrivas systematiskt, spårbart och med ständiga förbättringar.
- Planering, utbildning och övning ska vara en del av det förebyggande arbetet.
- Det ska finnas en förmåga att förebygga, upptäcka och hantera skadlig inverkan på Region Stockholms verksamhet.

Skyddsgärder ska samverka
Skyddsåtgärderna ska sammantaget:
- Förebygga att obehöriga får tillträde till byggnader, lokaler och anläggningar där skyddsvärd verksamhet bedrivs.
- Förebygga att personer som inte är pålitliga ur säkerhetssynpunkt arbetar i skyddsvärd verksamhet.
- Förebygga att informationstillgångar röjs, ändras, görs otillgängliga eller förstörs.
- Ge förmåga att hantera störningar och kriser så att kritiska verksamheter och processer kan upprätthållas.