Region Skånes revisorer

Fredrik Ljunggren
Certifierad kommunal revisor
fredrik.ljunggren@skane.se

MISSIV
Datum 2023-11-21--22
Dnr 2023-RG000030

Regionstyrelsen
Kollektivtrafiknämnden

Granskning av IT-säkerhet kollektivtrafiken - Rapport nr 4 – 2023

Den sammanfattande bedömningen är att kollektivtrafiknämnden inte har säkerställt att IT-säkerhetsarbetet är ändamålsenligt inom Skånetrafiken.

Region Skåne har ett ledningssystem för informationssäkerhet som inkluderar fastställda styrdokument i form av policys och riktlinjer för informationssäkerhetsarbetet som alla förvaltningar har att efterleva.

Ledningssystemet för informationssäkerhet är inte etablerat i tillräcklig utsträckning inom Skånetrafiken vilket har genererat en bristfällig kännedom om gällande styrdokument och krav. Det saknas därigenom etablerade processer och aktiviteter för IT-säkerhetsarbetet i enlighet med den struktur och systematik som arbetet ska bedrivas inom. Den ansvarsfördelning som är dokumenterad omsätts inte i praktiken och roller avseende IT-säkerheten för de system som nyttjas inom kollektivtrafiken är inte tydligt definierad.

I bilaga till detta missiv lämnar vi rekommendationer till regionstyrelsen och kollektivtrafiknämnden. I bilaga anges också instruktioner för yttrande samt svarsformulär.

Revisorskollegiet behandlade rapporten vid sammanträdet 2023-11-21--22 och beslutade att översända missiv och rapport för yttrande till ovan berörda nämnder/styrelser. Yttranden med uppgifter om verkställda och planerade åtgärder ska lämnas senast 2024-03-01.

För revisorskollegiet

Peter J Olsson
Ordförande

George Smidlund
Revisionsdirektör

Bilaga

Revisorernas rekommendationer

Rekommendationer till regionstyrelsen:

- Revidera styrdokument så att dessa är aktuella och utgör en ändamålsenlig styrning av informationssäkerhetsarbetet i Region Skåne.
- Säkerställa att ledningssystemet för informationssäkerhet etableras i samtliga verksamheter och att aktiviteter genomförs i enlighet med den systematik som beslutats.
- Utvärdera om organisation och funktioner är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska bedrivas.
- Säkerställa att regionstyrelsen i sin uppsiktsplikt stärker den interna kontrollen över efterlevnad av styrande dokument.

Rekommendationer till kollektivtrafiknämnden:

- Säkerställa att informationssäkerhetsarbetet genomförs i enlighet med beslutade krav och systematik.
- Säkerställa att roll- och ansvarsfördelning tydliggörs och etableras inom kollektivtrafiknämndens verksamheter.
- Säkerställa att kontinuitetsplaner för störning och avbrott upprättas för IT-system inom kollektivtrafiknämnden samt att övning och granskning genomförs i syfte att säkerställa ändamålsenlighet, aktualitet och kunskap.
- Säkerställa att informationsklassning och riskanalyser genomförs systematiskt på de informationstillgångar som hanteras i verksamheten samt att åtgärdsplaner upprättas utifrån erhållet resultat.
- Säkerställa att säkerhetsåtgärder vidtas i syfte att skydda informationstillgångar och för att minimera eller eliminera risker som identifierats samt att dessa utvärderas regelbundet.
- Säkerställa att gällande incidenthanteringsrutiner etableras samt att inträffade incidenter utgör del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.
- Säkerställa att den uppföljning som sker av informations-säkerhetsarbetet även inkluderar IT-säkerhet.
- Stärka den interna kontrollen avseende efterlevnad av styrdokument för informationssäkerhet.
- Säkerställa att nämnden erhåller återrapportering i tillräcklig utsträckning i syfte att kunna fatta beslut om erforderliga åtgärder för att stärka IT-säkerheten.

Anvisningar för yttrande

- Svaret ska innehålla uppgifter om vilka åtgärder som vidtagits eller planeras vidtas utifrån revisorernas rekommendationer.
- Det ska finnas en tydlig koppling mellan de rekommendationer som revisorerna lämnat och de åtgärder som beskrivs i svaret.
- Svaret bör så långt det är möjligt innehålla tidsangivelser för när åtgärderna genomförs.
- Svaret bör så långt det är möjligt innehålla beskrivning hur åtgärderna genomförs.
- Svaret bör så långt det är möjligt beskriva vilken eller vilka funktioner inom förvaltningen eller sjukhuset som fått i uppdrag att arbeta med åtgärderna.
- Om styrelsen/nämnden inte planerar att vida några åtgärder, motivera varför.
- Om styrelsen/nämnden inte kan svara på utsatt tid, kontakta revisionskontoret.

Nedan bifogas formulär som kan användas för svar på revisorernas rekommendationer. Syftet med formuläret är att underlätta kommunikationen och därmed tydliggöra vilka åtgärder styrelsen och nämnden vidtagit eller planerar att vidta.

Svarsformulär för regionstyrelsen

Revidera styrdokument så att dessa är aktuella och utgör en ändamålsenlig styrning av informationssäkerhetsarbetet i Region Skåne.
Regionstyrelsens svar:
Säkerställa att ledningssystemet för informationssäkerhet etableras i samtliga verksamheter och att aktiviteter genomförs i enlighet med den systematik som beslutats.
Regionstyrelsens svar:
Utvärdera om organisation och funktioner är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska bedrivas.
Regionstyrelsens svar:
Säkerställa att regionstyrelsen i sin uppsiktsplikt stärker den interna kontrollen över efterlevnad av styrande dokument.
Regionstyrelsens svar:
Övriga kommentarer:
Regionstyrelsens svar:

Svarsformulär för kollektivtrafiknämnden:

Säkerställa att informationssäkerhetsarbetet genomförs i enlighet med beslutade krav och systematik.
Kollektivtrafiknämndens svar:
Säkerställa att roll- och ansvarsfördelning tydliggörs och etableras inom kollektivtrafiknämndens verksamheter.
Kollektivtrafiknämndens svar:
Säkerställa att kontinuitetsplaner för störning och avbrott upprättas för IT-system inom kollektivtrafiknämnden samt att övning och granskning genomförs i syfte att säkerställa ändamålsenlighet, aktualitet och kunskap.
Kollektivtrafiknämndens svar:
Säkerställa att informationsklassning och riskanalyser genomförs systematiskt på de informationstillgångar som hanteras i verksamheten samt att åtgärdsplaner upprättas utifrån erhållet resultat.
Kollektivtrafiknämndens svar:
Säkerställa att säkerhetsåtgärder vidtas i syfte att skydda informationstillgångar och för att minimera eller eliminera risker som identifierats samt att dessa utvärderas regelbundet.
Kollektivtrafiknämndens svar:

Säkerställa att gällande incidenthanteringsrutiner etableras samt att inträffade incidenter utgör del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.
Kollektivtrafiknämndens svar:
Säkerställa att den uppföljning som sker av informationssäkerhetsarbetet även inkluderar IT-säkerhet.
Kollektivtrafiknämndens svar:
Stärka den interna kontrollen avseende efterlevnad av styrdokument för informationssäkerhet.
Kollektivtrafiknämndens svar:
Säkerställa att nämnden erhåller återrapportering i tillräcklig utsträckning i syfte att kunna fatta beslut om erforderliga åtgärder för att stärka IT-säkerheten.
Kollektivtrafiknämndens svar:
Övriga kommentarer:
Kollektivtrafiknämndens svar: