Myndigheten för samhällsskydd och beredskap

EXEMPEL

Informationssäkerhet ur ett styrningsperspektiv

– Informationssäkerhetsfunktion Organisatorisk placering

Informationssäkerhet ur ett styrningsperspektiv – Informationssäkerhetsfunktion Organisatorisk placering

Förslag som ingår i dokument som beskriver organisation och roller och ansvar.

Informationssäkerhetssamordnare regionledning

Den strategiske informationssäkerhetssamordnaren samordnar, leder och utvecklar arbetet med informationssäkerhet inom regionen.

Denne rapporterar löpande till regiondirektören samt årligen vid ledningens genomgång avseende informationssäkerhet.

Arbetsuppgifter och ansvar:

- Leda och ansvara för uppdraget inom strategisk arbetsgrupp för informationssäkerhet.
- *Vara sammankallande i Regionens informationssäkerhetsforum.*
- *Vara sammankallande i Regionens informationssäkerhetsråd.*
- *Verkställer samordningen av informationssäkerhetsarbetet och förvaltar de tillhörande riktlinjerna och tillämpningsanvisningarna samt den övergripande handlingsplanen för informationssäkerhet.*
- *Vid avsaknad av medel påvisa risken för att inte kunna utöva föreskrivet ansvar.*

IT-Säkerhetsansvarig regionledning

IT-säkerhetsansvarig, leder och utvecklar arbetet med IT säkerhet inom regionen. Har ett nära samarbete med Strategisk informationssäkerhetssamordnare och är en förlängd arm till organisationens it-verksamhet. Rollen ska vara drivande, normerande, stödjande och kontrollerande gentemot den egna organisationens it-produktion, och även gentemot externa leverantörer.

I uppgifterna ingår att:

- löpande initiera och genomföra säkerhetshöjande förbättringsåtgärder för IT-infrastrukturen, baserat på kraven för regionens verksamhetssystem
- handlägga auktorisationer av nya och uppgraderade IT-system för godkännande innan de anskaffas och införs i IT-miljön
- genomföra risk- och sårbarhetsanalyser av specifika delar i IT-miljön utifrån bl.a. ställda verksamhetskrav på informationssäkerhet
- löpande analysera och följa upp rapporterade IT-säkerhetsincidenter och utifrån dessa initiera säkerhetshöjande åtgärder
- vara konsultativ resurs för verksamheter som har behov av att utforma säkerhetshöjande åtgärder i IT-system
- agera kravställare säkerhet och säkerhetsrevisor på extern IT-driftleverantör som innehar avtal för regionens IT-drift
- samordna IT-säkerhetsarbetet gentemot regionens systemägare för att få enhetlig utformning och nivå på de olika verksamhetssystemens säkerhets-åtgärder/-funktioner
- bistå DSO med kompetens inom dataskydd t ex att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen.

Övergripande strategisk arbetsgrupp informationssäkerhet

Arbetsgruppen är regionledningens förlängda arm för informationssäkerhet och ska driva det regionövergripande informationssäkerhetsarbetet och vara stöd för regionledningen i informationssäkerhetsfrågor.

Grupperingen ingår i informationssäkerhetsrådet och är rådgivande i övergripande informationssäkerhetsfrågor utifrån aktiv omvärldsbevakning inom området. Gruppen leds av strategisk informationssäkerhetssamordnare.

Huvudsakligt uppdrag är att ge förutsättningar för ledning, verksamhetschefer och medarbetare att i sin tur ta ansvar för informationssäkerheten i sin verksamhet.

Huvudsakliga ansvarsuppgifter är indelade i följande områden:

Riskhantering

- Ta fram en strategi för omvärldsanalys och den egna organisationen avseende informationssäkerhet så att informationssäkerhetsarbetet kan bygga på en aktuell bild av krav (omvärldsanalys, ingångna avtal, författningar) och risker så att relevanta säkerhetsåtgärder kan beslutas.
- Verka för god medvetenhet och kunskap om informationssäkerhetsrisker genom en strategi för informations- och utbildningsaktiviteter gällande informationssäkerhet.
- Stödja informationsägare vid hantering av riskförteckning samt ha en övergripande bild av informationshanteringsrisker i regionen.

Planering och uppföljning

- Systematiskt arbeta för ständiga förbättringar bl.a. genom riskanalyser och granskningar inom området.
- Ta fram och underhålla en övergripande handlingsplan för informationssäkerhet för regionen som minst innehåller mål, beskrivning av aktiviteter, kostnader, ansvar samt start- och sluttider.
- Beredning av informationssäkerhetsfrågor för beslut av ledning (samordnas i rådet).
- Löpande uppföljning av beslutade åtgärder.
- Sammanställa verksamheternas utvärdering av informationssäkerhetsarbetet.
- Kontinuerlig lägesrapportering för regionens informationssäkerhetsläge till regiondirektören.
- Ansvara för genomförandet av ledningens genomgång för regionledningen.

Styrdokument

- Ta fram och underhålla regionens ledningssystem för informationssäkerhet, informationssäkerhetspolicy samt riktlinjer för informationssäkerhet. Har mandat att uppdatera styrdokument och genomföra ändringar som endast innebär mindre påverkan.
- Vara stödjande och rådgivande till DSO samt verksamheten gällande informationssäkerhet i dataskyddsfrågor.

Incidenthantering

- Bevaka och sammanställa central rapportering för informationssäkerhetsincidenter. Vid allvarliga informationssäkerhetsincidenter omedelbart rapportera till Säkerhetschef och vid behov regionens ledning.
- Rapportera incidenter och hantera samordning med IT och DSO ….

Utvärdering

- Ansvara för metoder och mallar för kontroll och granskning av informationssäkerheten.
- Initiera interna och externa revisioner för att:
  - utvärdera informationssäkerhetsarbetet inom regionen
  - följa upp efterlevnad av policyer, riktlinjer och rutiner gällande informationssäkerhet i regionen och vid behov föreslå förbättringar.

Samverkan och kommunikation

- Upprätthålla externa kontakter med relevanta myndigheter, granskningsorgan etc. rörande informationssäkerhetsfrågor.
- Förmedla expertstöd.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**