Myndigheten för samhällsskydd och beredskap

EXEMPEL

Informationssäkerhets-samordnare

– Region

Informationssäkerhets-samordnare

Informationssäkerhetssamordnare övergripande

Samordnar, leder och utvecklar arbetet med informationssäkerhet. Rapporterar löpande till högsta ledningen samt årligen vid ledningens genomgång avseende informationssäkerhet.

Arbetsuppgifter och ansvar:

- Verkställer samordningen av informationssäkerhetsarbetet och förvaltar de tillhörande riktlinjerna och tillämpningsanvisningarna samt den övergripande handlingsplanen för informationssäkerhet.
- Ansvarar för övergripande plan samt budget för området.
- Vid avsaknad av medel påvisa risken för att inte kunna utöva föreskrivet ansvar.
- Ordförande och sammankallande informationssäkerhetsrådet.
- Kontaktperson för övergripande frågor.

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 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.
- Medverka vid riskanalyser och konsekvensbedömningar.

Planering och uppföljning

- Systematiskt arbeta för ständiga förbättringar bland annat genom riskanalyser och granskningar inom området.
- Ta fram och underhålla en övergripande handlingsplan för informationssäkerhet som minst innehåller mål, beskrivning av aktiviteter, kostnader, ansvar samt start- och sluttider.
- Beredning av informationssäkerhetsfrågor för beslut av ledning.
- Löpande uppföljning av beslutade åtgärder.
- Sammanställa verksamheternas utvärdering av informationssäkerhetsarbetet.
- Kontinuerlig lägesrapportering för verksamhetens informationssäkerhetsläge till ledningen.
- Ansvara för genomförandet av ledningens genomgång för högsta ledningen.
- Årligen rapportera om informationssäkerhetsarbetet till ledningen.

Styrdokument

- Ta fram och underhålla organisationens ledningssystem för informationssäkerhet, informationssäkerhetspolicy samt riktlinjer för informationssäkerhet. Har mandat att uppdatera styrdokument och genomföra ändringar som endast innebär mindre påverkan. (Rutin och Instruktion) Riktlinjer beslutas av högsta ledningen.
- 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 högsta ledningen.
- 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
  - följa upp efterlevnad av policyer, riktlinjer och rutiner gällande informationssäkerhet i organisationen och vid behov föreslå förbättringar.

Samverkan och kommunikation

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

Vägledning från MSB. Ledningens roll inom informationssäkerhet.

https://www.informationssakerhet.se/siteassets/metodstod-for-lis/ledningens-roll-inom-informationssakerhet---ett-stod-for-dig-med-en-ledande-funktion.pdf

Den som driver en organisations informationssäkerhetsarbete kallas här, precis som i MSB:s metodstöd, för CISO – Chief Information Security Officer. Andra benämningar på rollen är informationssäkerhetschef, informationssäkerhets-samordnare eller informationssäkerhetsstrateg.

CISO:s uppdrag spänner över hela organisationen och innefattar allt ifrån att planera och anpassa informationssäkerhetsarbetet till att utifrån behov stötta ledningen och alla övriga roller som har ett informationssäkerhetsansvar i operativa, taktiska och strategiska frågor.

För att arbetet med informationssäkerhet ska bli bra behöver ledningen stöd av en CISO, som har till uppgift att driva arbetet i organisationen och vara ledningens kontaktpunkt i dessa frågor. CISO behöver rapportera direkt till och ha en god dialog med ledningen för att kunna göra ett bra jobb.

Informationssäkerhetssamordnare förvaltning – operativ nivå

Samordna, utveckla och följa upp informationssäkerhetsarbetet utifrån organisationens övergripande styrande dokument inom utsedd förvaltning.

Arbetsuppgifter och ansvar:

- Delta i potentiellt informationssäkerhetsråd.
- Ge stöd och delta i framtagande av övergripande styrande dokument såsom regler, metoder och tekniker avseende informationssäkerhet.
- Sprida kunskap om regler, styrande dokument, metoder och tekniker avseende informationssäkerhet i verksamheten.
- Ge stöd för intressentanalys, informationsklassning, riskanalys samt kravställning för de åtgärder som krävs för att skydda informationstillgångar.
- Samarbeta med dataskyddssamordnare med att stödja verksamheten vid genomförandet av informationsklassificering och olika typer av riskbedömningar inkluderande konsekvensanalyser avseende dataskydd enligt dataskyddsförordningen.
- Ge stöd i frågor gällande efterlevnad av interna riktlinjer och gällande lagkrav kopplat till informationssäkerhet. Informera förvaltningschefen/informationsägaren om legala krav inte efterlevs och vid behov rapportera till organisationens stödfunktioner.
- Ge stöd vid framtagandet av en handlingsplan för informationssäkerhet i verksamheten som följer organisationens övergripande handlingsplan.
- Ge stöd vid framtagande av lokala rutiner och arbetssätt vid hantering av information med anledning av verksamhetsspecifika informationssäkerhetsbehov.
- Ge stöd vid utveckling, förändring eller nyanskaffning och arbetet med leverantörsrelationer.
- Ge stöd inför, under och vid avslut av anställning.
- Ge stöd till verksamheterna och medarbetarna i frågor som rör informationssäkerhet.
- Ge stöd vid informationssäkerhetsincidenter. Sammanställa informationssäkerhetsincidenter och rapportera till central sammanställning.
- Samråda med dataskyddssamordnaren kring hantering av personuppgiftsincidenter och dataintrångsärenden inom förvaltningen.
- Ge stöd vid utvärdering och uppföljning av informationssäkerhetsarbetet.
- Ge stöd vid interna och externa revisioner.
- Årligen rapportera verksamhetens efterlevnad av informationssäkerhet av policy, riktlinjer och rutiner till informationsägare samt till strategisk informationssäkerhetssamordnare.

Myndigheten för
samhällsskydd
och beredskap

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