Myndigheten för samhällsskydd och beredskap

EXEMPEL

Riktlinje roller och ansvar inom lednings-system för säkerhet

– Region

Riktlinje roller och ansvar inom ledningssystem för säkerhet – Region

Enhet: CS-SI

Produktion: Advant

Innehåll

Syfte

Säkerhet är en förutsättning för att upprätthålla förtroendet från samhället, övriga intressenter eller personers vars integritet vi behöver skydda.

Vårt behov av säkerhet är beroende de uppdrag verksamheter har. Uppdrag kan framgå av lagar, förordningar eller politiska beslut. Uppdragen kan ingå i samhällsviktig eller säkerhetsskyddsklassificerad verksamhet och styras av exempelvis säkerhetsskyddslag och dataskyddsförordning.

I dessa uppdrag sker informationsbehandling i olika processer och för olika ändamål som innebär att information och de resurser som hanterar information ska skyddas utifrån de krav som ställs.

Omfattning

Säkerhetsarbetet inom Regionen berör områdena informationshantering, IT säkerhet, allmän och fysiskt teknisk säkerhet, krisberedskap. Regionen använder benämningen säkerhet vilket inbegriper begreppen informationssäkerhet, IT säkerhet och personsäkerhet.

Detta dokument fastställer organisation för säkerhetsarbetet.

Ledningssystem

Ett ledningssystem för säkerhet används för att ge inriktning, styrning samt leda en organisationens säkerhetsarbete och omfattar hela inom området för säkerhet. Ledningssystemet för säkerhet, LS utgår från säkerhetspolicyn.

Det innebär att ledningen på ett systematiskt sätt kan planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamheten.

Det systematiska och riskbaserade arbetet med säkerhet, sker enligt etablerade standarder med utgångspunkt i SS-ISO/IEC 27001. Det operativa arbetet bedrivs ute i verksamheterna genom utarbetade handlingsplaner och genom uppföljning av arbetet.

Ansvar

Regionfullmäktige

Regionfullmäktige fastställer policy för säkerhet.

Regionstyrelsen

Regionstyrelsen ger Regiondirektören i uppdrag att ansvara för omfattning och inriktning av säkerhetsarbetet.

Regiondirektör

Regiondirektören representerar högsta ledningen och har som tjänsteman det yttersta ansvaret för organisationens säkerhet. Ledningen uttrycker övergripande mål och inriktning för säkerhet i en säkerhetspolicy. Dessa dokument beslutas av regionfullmäktige.

Regiondirektören fastställer av organisation, regler och riktlinjer och följer upp Regionens säkerhetsarbete samt ta beslut om resursbehov vid förbättringsåtgärder för säkerhet som inte kan ombesörjas i ordinarie budget och verksamhetsplan.

Verksamhetsansvar

Ansvaret för säkerheten ska vara kopplat till det delegerade verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet också är ansvarig för säkerhet inom sin verksamhet. Det specifika ansvaret beskrivs närmare i styrdokument för ansvariga i linjen som kompletteras med styrdokument för systematiskt säkerhetsarbete.

Informationsägare

Den som äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

Eftersom skadeverkningarna av bristande säkerhet i informationsbehandlingsprocesser uppstår hos informationsägaren är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning. Informationsägaren är därmed riskägare för den information som ska hanteras av personal i exempelvis fysiska resurser eller IT resurser. Ägaren ansvarar för att det finns adekvat skydd för den information som lagras eller bearbetas av olika resurser. En resurs kan vara medarbetare, fysiska lokaler eller IT komponenter.

Dataskyddsombudet kan initiera riskbedömning avseende dataskyddet. Samordning inkluderar att genomföra DPIA tillsammans med dataskyddsombudet och informationsägaren.

Beroende på organisationsmodell är primärt verksamhetschef, avdelningschef eller förvaltningschef informationsägare.

Objektägare/systemägare

Alla resurser som hanterar, bearbetar eller lagrar information oavsett i analog eller digital form ska ha en ägare (objektägare). Om en objektägare i ett nuläge inte når upp till det efterfrågade skyddet ska detta kommuniceras till informationsägaren som får fatta beslut om åtgärder eller kvarstående risk.

Objektägaren har det övergripande ansvaret för det verksamhetsnära förvaltningsarbetet inom objektet.

I stora och medelstora organisationer är ofta den IT ansvarige ägaren för de infrastrukturella datorsystemen, ekonomichefen är ägare för ekonomisystemet, personalchefen är ägare för det personaladministrativa systemet, olika produktionschefer är ägare för respektive produktionssystem och så vidare.

Behov av skyddsnivå kan innebära att infrastruktur, stödsystem får ett högre behov av skyddskrav, dvs aggregering, än de verksamhetssystem de stödjer. Ägarens uppgift är att IT verksamheten implementerar tillräcklig skyddsnivå över hela IT-resursens livscykel (införande, under drift och vid avveckling).

Arkivchef

Ansvarar för att säkerställa skyddet för arkiv av informationstillgångar som ska arkiveras. Reglerar uppdraget i verksamhetens arkivredovisning med instruktion samt struktur för informationshanteringsplaner. Arkivredovisning med tillhörande informationshanteringsplaner utgör i huvudsak det övergripande register som krävs för informationstillgångar i enlighet med ISO 27001. Detta register kan även utgöra regionens förteckning över personuppgiftsbehandlingar.

Digitaliseringsansvarig eller projektledare

Rollerna ansvarar för att leda genomförandet av nya initiativ eller olika typer av förändringar där känslig information kan hanteras. Bedömning av informationssäkerhetsrisker ska tidigt vara en integrerad del i projekt och hanteras regelbundet för att minska risken för obehörig tillgång, spridning av information eller att säkerhetsincident uppstår. Initiativ skall arbeta i enlighet med riktlinjer avseende säkerhet i allmänhet men specifikt avseende anskaffning och systemutveckling, samt hanteringsregler.

Om initiativ kommer hantera känsliga personuppgifter kan en DPIA (Data protection impact assessment). Om initiativ ska hantera personuppgiftbehandlingar ska krav från styrande dokument gällande dataskydd användas i projektstyrningen.

Jurist

Juristen har följande ansvar inom området Juridik:

- Ge stöd avseende sekretessbedömningar.
- Fatta beslut vid utlämnande av handling.

Chef HR

Utöver det ansvar som varje chef har för informationssäkerhet tillkommer följande ansvar för området HR:

- Säkerställa att det finns processer och rutiner för att verifiera sökande personers pålitlighet och lämplighet vid anställning.
- Initiera säkerhetsprövning innan person börjar sin anställning.
- Upprätta tillämpliga avtal med medarbetare för att säkerställa informationssäkerhet.
- Säkerställa att det finns process och information som inbegriper informationssäkerhetsaspekter att följa vid avslutad anställning (avrustning).

Delegation av ansvar och utförande

Det ansvar som åligger chef kan och bör delegeras till lämpliga roller i verksamheten. Vid delegation behöver ansvar och uppgifter från övriga styrande dokument för informationssäkerhet fördelas. Specialistfunktioner och stödjande roller kan med fördel vara involverade i verksamhetens/förvaltningens säkerhetsarbete.

Specialistfunktioner med övergripande ansvar för säkerhetsarbetet

Säkerhetschef (CSO)

Säkerhetschef (Chief Security Officer, CSO) har utöver det ansvar som varje chef ett specifikt ansvar för att driva och leda det regionövergripande säkerhets- och beredskapsarbetet och vara stöd för regionledningen i säkerhetsfrågor.

Huvudsakligt uppdrag är att ge förutsättningar för ledning, verksamhetschefer och medarbetare att i sin tur ta ansvar för säkerhet- och beredskap i egen verksamhet.

Säkerhetschefens huvudsakliga ansvar:

- Rapporterar till regiondirektören löpande vid behov samt årligen vid ledningens genomgång avseende säkerhet.
- Har under regiondirektören det övergripande ansvaret för att regionens säkerhetsarbete bedrivs enligt gällande författningar och interna styrdokument.
- Aktivt stödja regiondirektören så att han eller hon kan fullfölja sitt ansvar för verksamheten, ekonomi och personal.
- Ansvar för att hålla samman regionens riskregister för krisberedskap och civilt försvar. (RSA)

Säkerhetschefen har delegerat ansvaret för strategisk styrning och uppföljning av säkerhetsarbetet vilket inkluderar administrativ samt teknisk säkerhet till en strategisk säkerhetsfunktion.

Övergripande strategisk säkerhetsfunktion

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

Funktionen har det delegerade ansvaret för att:

- förvalta och utveckla ledningssystemet och de tillhörande riktlinjerna och tillämpningsanvisningarna inom området för regionen
- följa upp och kontrollera regionens säkerhetsarbete
- samordna utvärdering och rapportering av säkerhetsarbetet
- ta fram övergripande handlingsplaner samt budget för regionens säkerhetsarbete.

Funktionen ingår i informationssäkerhetsrådet och är rådgivande i övergripande informationssäkerhetsfrågor utifrån aktiv omvärldsbevakning inom området.

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

- Förvaltar och utvecklar ledningssystemet för säkerhet i enlighet med ISO 27001. 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.
- Analysera och följa upp rapporterade säkerhetsincidenter och utifrån dessa initiera säkerhetshöjande åtgärder.
- Rapportera incidenter och hantera samordning med 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.

Säkerhetsstrateg (CISO)

Regionens säkerhetsstrateg samordnar, leder och utvecklar arbetet med säkerhet inom regionen och är ett stöd för regionledningen i säkerhetsfrågor.

Strategen rapporterar löpande till säkerhetschefen samt gemensamt till regiondirektören årligen vid ledningens genomgång avseende informationssäkerhet.

Arbetsuppgifter och ansvar:

- Verkställer samordningen av informationssäkerhetsarbetet dess styrning och uppföljning.
- Utvärderar styrning och effekt av processer som ingår i ledningssystemet.
- Ingår i den strategiska säkerhetsfunktionen.
- Är sammankallande för Regionens informationssäkerhetsforum.
- Är sammankallande för Informationssäkerhetsrådet.
- I rollen ingår att medverka vid risk- och sårbarhetsanalyser samt utbildnings- och informationsinsatser inom området.
- Vid avsaknad av medel påvisa risken för att inte kunna utöva föreskrivet ansvar.

IT-Säkerhetsansvarig

IT-säkerhetsansvarig utvecklar IT säkerhetsarbetet inom regionen. Har ett nära samarbete med säkerhetsstrateg och är en förlängd arm till organisationens it-verksamhet men är inte operativ utförare eller ansvarig för genomförande av åtgärder.

Arbetsuppgifter och ansvar:

- Ingår i den strategiska säkerhetsfunktionen.
- Har löpande dialog med samtliga IT-förvaltningar inom regionen kring de rutiner och krav som gäller inom IT-säkerhetsområdet.
- Rådgivande i övergripande IT-säkerhetsfrågor om relevanta säkerhetsåtgärder för IT-verksamheten.
- Involvera IT-arkitekter och systemförvaltare vid implementering av teknisk lösning.

- Bedriva aktiv omvärldsbevakning inom området.
- Medverka vid risk- och sårbarhetsanalyser samt utbildnings- och informationsinsatser inom området.
- Övergripande ansvar för att register hålls över IT tekniska tillgångar.
- Utvärdera säkerheten i den egna organisationens it-produktion, samt externa leverantörer.
- Vid avsaknad av medel påvisa risken för att inte kunna utöva föreskrivet ansvar.

Fysisk säkerhetsansvarig

Specialist inom fysisk säkerhet samordnar arbetet med fysisk säkerhet och har ett nära samarbete med säkerhetsstrateg och är en förlängd arm till fastighetsservice samt trygghetscentral men är inte operativ utförare eller ansvarig för genomförande av åtgärder.

Fysisk säkerhet omfattar utrustning, lokaler samt försörjningssystem. Rollen innebär att ha kompetens inom skalskydd, fysiskt skydd av mobila enheter, kablage, brandskydd, underhåll och kontinuitet samt destruktion.

Arbetsuppgifter och ansvar:

- Ingår i den strategiska säkerhetsfunktionen.
- Har löpande dialog med samtliga förvaltningar inom regionen kring de rutiner och krav som gäller inom säkerhetsområdet.
- Rådgivande i övergripande säkerhetsfrågor för fysiskt skydd.
- Bedriva aktiv omvärldsbevakning inom området.
- Medverka vid risk- och sårbarhetsanalyser samt utbildnings- och informationsinsatser inom området.
- Övergripande ansvar för att register hålls över fysiska tillgångar.
- Utvärdera säkerheten för den egna organisationens fysiska tillgångar, samt hos externa leverantörer.
- Vid avsaknad av medel påvisa risken för att inte kunna utöva föreskrivet ansvar.

Roller och ansvar i förhållande till säkerhetsskydd

Enligt säkerhetsskyddslagen ska den som är ansvarig för en säkerhetskänslig verksamhet bl a se till att behovet av säkerhetsskydd utreds och att åtgärder planeras och vidtas inom informationssäkerhet, fysisk säkerhet och personalsäkerhet. Regionens verksamhet kräver att det finns en säkerhetsskyddschef som ska kontrollera att verksamheten bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen.

Regionen har ansvaret för efterlevnaden av Säkerhetsskyddslagen.

Detta ansvar innebär att:

- tilldela roller och ansvar för verksamhet som kräver säkerhetsskydd
- tillhandahålla tillräckliga resurser för att upprätthålla säkerhetsskyddet
- säkerställa säkerhetsskyddschefens oberoende ställning.

Säkerhetsskyddschef

Säkerhetsskyddschefen ska övervaka regionens arbete med säkerhetsskydd. Säkerhetsskyddschefen är och ska vara direkt underställd Regiondirektören.

Säkerhetsskyddschefens huvudsakliga ansvar:

- Är ansvarig för att regionens säkerhetsskydd bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen (2018:585) och Säkerhetsskyddsförordning (2018:658).
- Ansvarar för regionens säkerhetsskyddsanalys enligt 2 kap. 1§ säkerhetsskyddslagen (2018:585) och säkerhetsskyddsplan.
- Följer upp aktuell hotbild, presenterar förändringar till verksamheter inom regionen som lyder under säkerhetsskydd. Säkerhetschefen uppdaterar även säkerhetschefen och Regionledningsdirektören vid behov.
- Sammanhåller regionens säkerhetsrapportering och vidtar efter beredning inom regionen lämpliga säkerhetsskyddsåtgärder.
- Ansvarar för regionens internkontrollplan. Planerar och genomför regionens internkontroller vad avser säkerhetsskydd.
- Ansvarar för regionens analys av befattning samt anställdas inplacering i säkerhetsklass.

Signalskyddsansvarig

Ansvarig för regionens signalskydd/ kommunikationssäkerhet.

- Ansvarar för regionens signalskyddsinstruktion.
- Leder regionens interna utbildning i signalskydd.

Roller och ansvar i förhållande till krisberedskap

Krisberedskapshandläggare

Krisberedskapshandläggaren ska stödja säkerhetschefen med planering och samordning av krisberedskap och åtgärder inför höjd beredskap samt verka för en god krisberedskap och utveckla krisledningsorganisationen.

Krisberedskapshandläggaren delar i det övriga säkerhetsarbetet på enheten som bl.a. omfattar informationssäkerhet och inkluderar säkerhetsskydd.

I uppgiften ingår följande ansvar:

- Delta i risk- och sårbarhetsanalyser för att identifiera risker och utvecklingsbehov avseende regionens förmåga till krisberedskap samt åtgärder vid höjd beredskap.
- Ta fram åtgärdsplan för krisberedskap samt driva förändringsarbete internt och externt.
- Utveckla, planera och genomföra utbildnings- och övningsverksamhet.
- Delta i arbetet med kontinuitets- och krisplaner inklusive kriskommunikation.
- Delta i nätverk och samverkan med andra regioner, näringsliv, myndigheter, länsstyrelser, kommuner och frivilligorganisationer.
- Arbeta aktivt med omvärldsbevakning och ha samlad och aktuell kunskap inom området.

Roller och ansvar i förhållande till dataskydd

Regionen har ansvaret för efterlevnaden av Dataskyddslagen. Detta ansvar innebär att:

- tilldela roller och ansvar för verksamhet som kräver dataskydd
- tillhandahålla tillräckliga resurser för att upprätthålla dataskyddet
- säkerställa dataskyddsombudets oberoende ställning.

Dataskyddsombud, DSO

Dataskyddsombudet är en självständig och oberoende stöd- och kontrollfunktion.

Dataskyddsombudets uppgifter är enligt dataskyddsförordningen bland annat att informera och ge råd om vilka skyldigheter som gäller enligt såväl dataskyddsförordningen som andra nationella dataskyddsbestämmelser, bevaka att dessa regler följs och ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt förordningen.

Ombudet ska också fungera som kontaktpunkt för dataskyddsmyndigheten och samarbeta med denna.

Dataskyddsombudet har en självständig position och ska i frågor som rör behandling av personuppgifter kunna rapportera direkt till den del av organisationen som dataskyddsombudet bedömer vara lämpligt för att möjliggöra sin uppgift.

I arbetsuppgifterna ingår bland annat att:

- delta i regionalt informationssäkerhetsråd
- informera, ge råd och stöd till personuppgiftsansvarig, handläggare och övrig personal
- vara tillgänglig för frågor från registrerade personer
- rapportera till högsta förvaltningsnivå om organisationens brister och utvecklingsbehov gällande att uppnå en korrekt och laglig personuppgiftsbehandling
- fungera som kontaktpunkt för tillsynsmyndigheten för dataskydd och vid behov genomföra förhandssamråd
- göra anmälan till tillsynsmyndigheten om brister inte åtgärdas.
- säkerställa att det finns en sammanställning (registerförteckning) över behandlingar av personuppgifter utifrån inlämnade register från respektive personuppgiftsansvarig
- övervaka regionens efterlevnad av dataskyddsförordningen och bevaka att registrerades rättigheter efterlevs
- bistå i utredning av misstänkta överträdelser och personuppgiftsincidenter och bedöma om inträffade incidenter ska anmälas till tillsynsmyndigheten

- bedöma handläggning för inkomna ärenden avseende t ex registerutdrag, klagomålshantering
- bistå registerägare och informationsägare med att identifiera rätt skyddsåtgärder för personuppgifter baserat på informationsklassning
- tillsammans med sakkunniga inom regionen kravställa och arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen
- tillsammans med sakkunniga ge råd vid genomförande av konsekvensbedömning för dataskydd och övervaka genomförandet av åtgärder som baseras på denna bedömning
- tillhandahålla och bevaka en funktionsbrevlåda (dataskydd@) dit frågeställningar kan skickas både av interna och externa intressenter.

Roller och ansvar i förhållande till krav inom Hälso- och sjukvård

Vårdgivare är den som har ett ansvar att bedriva hälso- och sjukvård enligt (HSLF-FS 2020:56) och ska ha ett ledningssystem för systematiskt kvalitetsarbete med processer och rutiner för informationssäkerhet enligt HSLF-FS 2016:40.

Grundläggande är att vårdgivaren ska identifiera, beskriva och fastställa de processer i verksamheten som behövs för att säkra verksamhetens kvalitet samt för att kunna tillämpa rätt skydd för informationstillgångar som ingår i dessa processer.

SOSFS 2011:9 Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete är tillämplig för verksamhet som styrs av följande lagstiftningar:

1. 5 kap. 4 § hälso- och sjukvårdslagen (2017:30),
2. 16 § tandvårdslagen (1985:125),
3. 6 § lagen (1993:387) om stöd och service till vissa funktionshindrade, LSS, och
4. 3 kap. 3 § tredje stycket socialtjänstlagen (2001:453). (HSLF-FS 2017:12)

Informationssäkerhetssamordnare Hälso- och sjukvård

Informationssäkerhetssamordnaren för hälso- och sjukvård ska stödja i analys och implementering av säkerhetsåtgärder.

Minst en gång om året ska detta arbete rapporteras till vårdgivaren. Sammanställningen ska innehålla information om:

- riskanalyser som har gjorts av informationssäkerheten
- incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada
- uppföljningar som har gjorts
- förbättringsåtgärder som har vidtagits.

Operativ säkerhet

Informationshantering – förvaltning

Förvaltningsledare

Förvaltningsledare är huvudansvarig förvaltare för hela förvaltningsobjekt och har ansvar för att verkställa de behov och krav som verksamheten har på objektet och tillhörande rutiner.

Utför på uppdrag av objektägare ledningsuppgifter för förvaltningsobjektet på motsvarande sätt som en projektledare för ett projekt. Utarbetar förvaltningsplan tillsammans med förvaltningsledare IT.

Ansvar och befogenheter:

- Att utarbeta förvaltningsplan.
- Att verkställa förvaltningsplanens mål inom givna ramar på ett kostnadseffektivt sätt.
- Att prioritera, besluta, planera, genomföra och följa upp aktiviteter inom ramen för förvaltningsplanen.
- Att personal som hanterar informationsresurser får instruktioner om hur de hanterar dessa, vilka villkor och vilket ansvar som gäller samt den information de får åtkomst till (oavsett om det är intern eller extern personal).
- Att avropa mot ingångna avtal.
- Att godkänna leveranser från IT-parter.
- Att upprätta löpande förvaltningsdokumentation och rapporteringsrutiner.
- Att kontinuerligt rapportera status, avvikelser och uppföljning av kostnader till objektägare och styrgrupp.

Informationssäkerhetssamordnare förvaltning

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

Arbetsuppgifter och ansvar:

- Delta i regionalt informationssäkerhetsråd.
- Ge stöd och delta i framtagande av regionövergripande 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 regionala stödfunktioner.
- Ge stöd vid framtagandet av en handlingsplan för informationssäkerhet i verksamheten som följer regionens 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.

Fysisk säkerhet – förvaltning

Säkerhetssamordnare/Objektägare Lokaler

Lokal samordnare för fysisk säkerhet. Ansvarar för att säkerheten i lokaler uppfyller verksamhetens krav för skydd av information. Ett lokalobjekt kan vara särskilda utrymmen såsom datorhall, arkiv, korskopplingsrum mm.

I detta ansvar ingår att:

- säkerställa att lokaler har ett tillräckligt fysiskt skydd, i enlighet med verksamhetens behov samt att omhänderta de tillkommande krav för på fysiskt skydd som verksamheten ställer utifrån informationssäkerhet
- vid behov, ta fram kompletterande säkerhetsinstruktioner för lokalerna till stöd för regionens verksamhet
- säkerställa att personal endast har de inpasseringsbehörigheter som krävs för att utföra sina arbetsuppgifter
- säkerställa att personal och externa parter som nyttjar eller utför arbete och underhåll i regionens lokaler har tillräcklig utbildning för att det fysiska skyddet ska kunna upprätthållas
- ta fram lokal plan för SBA
- leda årlig utbildning i brandutrymning
- utföra regelbunden uppföljning av lokalernas säkerhet.

IT säkerhet – förvaltning

Förvaltningsledare IT

Utför, på uppdrag av objektägare IT, ansvarsuppgifter för förvaltningsobjektet vid sidan av förvaltningsledare med särskilt ansvar för de tekniska sambanden.

Omsätta funktionella krav från verksamheten till bästa möjliga tekniska lösning samt se till att förändringarna passar in i den tekniska miljön. t.ex. kravhantering, interaktionsdesign, testledning, teknisk dokumentation, drift och systemutveckling.

I ansvaret ingår att se till att tekniska sårbarheter identifieras, sårbarheter övervakas, sårbarheter riskbedöms, att uppdateringar av system sker samt att samordning som krävs utförs.

Ansvar och befogenheter:

- Att medverka vid RSA för berörda system.
- Att hålla och uppdatera register över alla IT system som behandlar information (Registrera avtal, systembeskrivning och systemförvaltningsorganisation).
- Att upprätta förvaltningsplan inkluderande tidplan för regelbundet återkommande underhåll, till exempel säkerhetsuppdateringar, hantering av säkerhetskopiering, övervakning, felsökning och åtgärder.
- Att verkställa förvaltningsplanens IT-relaterade mål på ett kostnadseffektivt sätt.
- Att IT-stöden är tillgängliga för verksamheten enligt överenskommen nivå.
- Att tillse att drifts-, support- och serviceavtal för aktuella IT-stöd finns upprättat och är aktuella.
- Att ha kontakt med de leverantörer som styrs med hjälp av kontrakt.
- Att tekniska samband fungerar tillfredsställande.
- Att säkerställa att kontinuerliga acceptanstester genomförs.
- Att definiera roller i systemen utifrån verksamhetsbehov, administrera behörigheter och tillhörande rutiner behörighetsrutiner och administrativa rutiner för beställning/borttag finns och är kända av IT-support och/eller extern driftsleverantör.
- Att användarhandböcker finns tillgängliga och är uppdaterade.
- Att bistå med kompetens vid gallring ser till att gallringsutredningar utförs för den information som finns lagrad, att gallringsfrister fastställs samt att systemet klarar arkiveringskrav.

IT – säkerhetstekniker

IT-säkerhetstekniker ska stödja vid beslut om relevanta säkerhetsåtgärder för IT-verksamheten och involvera IT-arkitekter och systemförvaltare vid implementering av teknisk lösning.

IT-säkerhetstekniker ska stödja IT-säkerhetsansvarig med att ge råd och följa upp IT-säkerhet för hela regionen.

IT-säkerhetstekniker ansvarar för att:

- kontinuerligt rapportera om IT-säkerhetsfrågor till IT-säkerhetsansvarig samt till säkerhetsstrategen
- följa regionens utveckling så att IT-säkerhetsarbetet kan bygga på en aktuell bild av krav (omvärldsanalys, ingångna avtal, författningar) och risker så att relevanta säkerhetsåtgärder kan beslutas
- stödja teknisk analys och riskbedömning för regionens IT verksamhet inklusive säkerhetsskyddsanalys enligt säkerhetsskyddslagen
- ta fram lösningsförslag i enlighet med kravställning avseende IT säkerhetsåtgärder både i egen drift och bedöma realisering hos externa leverantörer
- stödja IT verksamhetens kontinuitetshantering för tekniska plattformar
- stödja IT-säkerhetsansvarig och säkerhetsstrategen genom att verka för god medvetenhet gällande IT-säkerhet och IT-säkerhetsrisker
- stödja IT-säkerhetsansvarig med att följa upp IT-säkerhetsarbetet inom regionen
- omvärldsbevaka och upprätthålla externa kontakter rörande IT-säkerhetsfrågor.

Specifikt ansvar för följande områden:

- Härdning av operativsystem och applikationer.
- Logghantering och uppföljning.
- Perimeterskydd och regelverk för nätverkskommunikation.

Driftschef

Ansvarar för driften av IT-infrastrukturen. Tillhandahåller en plattform för installationen av systemet till systemadministratören.

Nätverksägare

Ansvarar för säkerhetsarkitektur samt förvaltning av nätverket. Beslutar/godkänner vilka system/resurser/tjänster som får anslutas till nätverket. Beslutar/godkänner konfiguration av brandväggar, switchar och annan utrustning som påverkar säkerheten. Säkerställer att nödvändiga penetrationstester genomförs. Säkerställer att eventuella intrång detekteras och åtgärdas.

Forum

Informationssäkerhetsforum

Forumet ska verka för en ökad kunskap och ett ökat informationssäkerhetsmedvetande ute i regionen. Forumet ska vara stöd för att hantera frågor utifrån verksamhetschefernas ansvar för informationssäkerhet i deras uppdrag.

Forumet ska fånga upp och samordna säkerhetsrelaterade behov i förvaltningarna. Forumet fungerar även för att kommunicera ut regionövergripande styrning inom området.

Forumet ska bistå verksamhet med kompetens inom dataskydd t ex att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen.

I Informationssäkerhetsforumet ingår roller som har ett ansvar för informationssäkerhet såsom verksamhetschefer, informationsägare, objektägare, projektledare, verksamhetsutvecklare, IT arkitekter och stödjande specialistroller.

Informationssäkerhetsråd

Informationssäkerhetsrådet ska vara verksamhets- och sakkunnigt stöd inom informationssäkerhetsområdet och ska bistå verksamhetscheferna i deras uppdrag samt vara remissinstans för regionens verksamheter i informationssäkerhetsfrågor.

Samtliga medarbetare i Regionen äger möjlighet att väcka ärenden till rådet.

Rådet ska bidra till ett processorienterat arbetssätt avseende säkerhetsfrågor inom området informations- och IT säkerhet.

Rådet ska ha företrädare med kompetens och funktionsansvar inom:

- juridik
- personuppgiftsbehandling och dataskydd
- riskhantering
- patientsäkerhet
- IT-säkerhet
- informationssäkerhet
- vårdadministrativt system, COSMIC
- krisberedskap
- säkerhetsskydd
- fysiskt skydd
- digitaliseringsuppdrag.

Andra företrädare för t ex arkiv, diarium, dokumenthantering, systemansvariga, kvalitetsutveckling kan adjungeras efter behov.

Sammankallande för informationssäkerhetsrådet är säkerhetsstrategen.

Huvudsakliga uppgifter:

Styrdokument

- Utifrån övergripande regler för informationssäkerhet lyfta fram förslag till nya.
- Utifrån fastställda regler, ge förslag på lokala rutiner som ska finnas tillgängliga i ledningssystemet.

Kravställning

- Utifrån övergripande styrning ge råd kring säkerhetskrav vid upphandling och införande av nya system samt bevaka uppfyllande av säkerhetskrav vid drift av system, datorer och nät.
- Vara stödjande och rådgivande till verksamheten gällande dataskyddsfrågor t ex avseende att kravställa, identifiera och ge förslag till säkerhetsåtgärder samt processer enligt principer för dataskydd.

Förbättringsarbete

- Initiera och bistå vid säkerhetsrevisioner.
- Delta i framtagandet och implementering av metoder och mallar för kontroll och granskning av informationssäkerheten.

Incidenthantering

- Hantera samordning av incidenter med IM Incident Manager och TIB.

Samverkan och kommunikation

- Fungera konsultativt som stöd och remissinstans för regionens verksamheter i informationssäkerhetsfrågor.
- Medverka vid arbetsplatsträffar eller liknande.
- Förmedla expertstöd (eget eller externt).
- Ge stöd till utbildningsinsatser och sprida information.

Omvärldsbevakning

- Sprida information från omvärldsbevakning.
- Delaktig i strategi kring omvärldsbevakning.

Uppföljning säkerhet

Uppföljning av säkerhetsläget, fastställda mål och handlingsplaner ska ske regelbundet vid ledningens genomgång vilket ska ske i varje verksamhet samt på aggregerad nivå till regiondirektör samt Regionfullmäktige.

Följsamheten till riktlinjer och regelverk ska regelbundet följas upp. Ett antal områden kräver uppföljning av efterlevnad med anledning av legal kravställning. För att bevaka efterlevnad har ansvaret delats ut till särskilda befattningshavare, såsom säkerhetschef, beredskapschef, säkerhetsskyddschef, dataskyddsombud, informationssäkerhetssamordnare. Till sitt stöd används analyser för att identifiera risker och lämpliga åtgärder utifrån respektive område för efterlevnad. Dessa analyser sker inom ramen för risk och sårbarhetsanalyser, säkerhetsskyddsanalys samt konsekvensbedömning dataskydd.

Myndigheten för
samhällsskydd
och beredskap

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