Regionshuset
Viborg

Region Midtjylland

Skottenborg 26
Postboks 21
DK-8800 Viborg
Tel. +45 7841 0000
kontakt@rm.dk
www.rm.dk

Bilag til fællesregional informationssikkerhedspolitik

Dato 13-03-2024
Rikke Stein
Tel. +4521359030
rikke.stein@rm.dk
1-16-02-13-08

Der arbejdes systematisk med informationssikkerhed i Region Midtjylland. Region Midtjylland er en politisk ledet organisation, hvor regionsrådet beslutter den politiske retning og de økonomiske rammer. Regionsrådet udstikker rammen for informationssikkerhed gennem den til enhver tid vedtagne informationssikkerhedspolitik.

Det vedlagte bilag har til formål at supplere den fællesregionale informationssikkerhedspolitik, som blev vedtaget af Regionsrådet den 24. august 2016. Bilaget beskriver organiseringen af arbejdet med informationssikkerhed og fastlægger, i samarbejde med politikken, både ansvarsplacering og rammer for dette arbejde i Region Midtjylland.

Risikobaseret tilgang
Region Midtjyllands strategiske tilgang til arbejdet med informationssikkerhed er risikobaseret. Den risikobaserede tilgang til informationssikkerhed betyder grundlæggende, at ressourcer er begrænsede, og at ikke alle risici kan elimineres fuldstændigt. Regionen har fokus på at identificere, vurdere og forstå de risici, som organisationen står overfor, for så at kunne prioritere blandt disse risici, således at regionen håndterer de væsentligste risici først.

Ved at fokusere på de mest kritiske trusler og sårbarheder og implementere passende foranstaltninger kan regionen opnå en mere effektiv beskyttelse af følsomme data og opretholde en sund balance mellem sikkerhed og organisatorisk drift. Den risikobaserede tilgang skal være med til at sikre, at regionen får mest mulig sikkerhed for de tilgængelige ressourcer.

Organisering

Informationssikkerhedsudvalget (ISU)
ISU udgør det strategiske niveau for arbejdet med informationssikkerhed. Udvalget træffer de overordnede

administrative beslutninger vedrørende informationssikkerhed i Region Midtjylland. Udvalget består af hele Direktionen, to ledelsesrepræsentanter fra forretningen, it-direktøren, it-sikkerhedschefen (CISO), vicedirektøren for Regionssekretariatet og regionens Databeskyttelsesrådgiver.

Alle sikringsforanstaltninger, som besluttes af ISU, er basisforanstaltninger, der som udgangspunkt ikke kan fraviges og skal overvåges og håndhæves af Informationssikkerhedsledelsen (ISL). Undtagelser og fravigelser skal forelægges ISU, der i særlige tilfælde kan give dispensation. Informationssikkerhedsudvalget kan også delegere dispensationsretten, såfremt der er tale om en midlertidig fravigelse. Informationssikkerhedsledelsen (ISL) er tildelt denne dispensationsret.

Styregruppen for informationssikkerhed (SFI)
Styregruppen for informationssikkerhed skal bidrage til at sikre ledelsens involvering samt synliggøre ledelsens ansvar for informationssikkerhed i organisationen. Styregruppen spiller en vigtig rolle som sparringspartner i forhold til at vurdere forretningens behov og især hospitalernes og socialområdets behov for at blive informeret og involveret i de tiltag, der iværksættes for at styrke regionens informationssikkerhed.

Styregruppen skal være med til at sikre, at informationssikkerhed forankres i hele organisationen. Derfor skal gruppens sammensætning afspejle en bred organisatorisk repræsentation og udpeges på ledelsesniveau med mandat til at repræsentere den enhed, medlemmerne kommer fra. SFI sammensættes derfor af ledelsesrepræsentanter både fra de afdelinger, der er udførende, samt fra den øvrige del af organisationen.

Informationssikkerhedsledelsen (ISL)
Den overordnede styring af informationssikkerhedsindsatsen koordineres af den samlede Informationssikkerhedsledelse. Dette er en fælles funktion mellem Regionssekretariatet og Digitalisering og It, og ISL har ledelsesansvaret for den samlede informationssikkerhedsfunktion, herunder at sørge for ledelse af medarbejdere og sikring af at ressourcer bliver varetaget bedst muligt.

ISL har ansvaret for Region Midtjyllands risikostyring inden for informationssikkerhed og arbejder derfor på vegne af ISU. ISL er ansvarlig for at håndtere opståede risici i overensstemmelse med den øverste ledelses risikoappetit og skal sikre et velfungerende og koordineret risikostyringssystem. For at kunne varetage denne opgaveportefølje kræves dialog og samarbejde med ISU, samt et delegeret mandat til i visse tilfælde at kunne handle på vegne af ISU.

Herunder varetager ISL muligheden for at i særlige tilfælde at kunne give midlertidige dispensationer. Alle medlemmer af ISL har mandat til at underskrive databehandleraftaler på vegne af Region Midtjylland som dataansvarlig og databehandler samt at underskrive sikkerhedsrelaterede aftaler, revisionserklæringer og lignende.

Informationssikkerhedsfunktionen (ISF)
På operationelt plan er der etableret en informationssikkerhedsfunktion i Region Midtjylland. Region Midtjyllands informationssikkerhedsfunktion er en fælles funktion mellem Regionssekretariatet og Digitalisering og It. Funktionen er koordinerende og drivende for arbejdet med informationssikkerhed i Region Midtjylland. Informationssikkerhedsfunktionen ledes på tværs af Informationssikkerhedsledelsen (ISL).

Informationssikkerhedsfunktionen skal på det operationelle niveau understøtte Informationssikkerhedsledelsen i at udmønte det besluttede sikkerhedsniveau. Opgaverne løftes i et samspil, men de enkelte kontorer har hver deres fokusområder.

Fra Regionssekretariatet indgår Den databeskyttelsesretlige enhed (herefter DBE) og Digital Forvaltning. DBE har fokus på juridisk rådgivning omkring databeskyttelseslovgivningen, herunder hjemmelsvurdering, rådgivning om databeskyttelsesretlige roller, udarbejdelse af databehandleraftaler/EU-standardkontrakter, risikovurderinger for den registrerede, sandsynlighedsvurdering ved tredjelandsoverførsler, tilsyn med regionens databehandlere og brud på persondatasikkerheden.

Digital Forvaltning bidrager til den overordnede styring af regionens informationssikkerhedsindsats og compliance på området. Kontoret løfter blandt andet følgende opgaver: udarbejdelse og formidling af politikker og retningslinjer, rådgivning omkring informationssikkerhed, udarbejdelse af risikovurderinger og konsekvensanalyser (DPIA), koordinering af regionens awarenessindsats og sekretariatetsbetjening af mødefora på området.

Sikkerhed & Compliance og Operationel Sikkerhed i ISF: Formålet med disse områder er at identificere, analysere og mitigere it-sikkerhedsmæssige risici. Dette sikres gennem overvågning af trusler og sårbarheder i infrastrukturen, udarbejdelse af risikovurderinger og retningslinjer, samt rådgivning om sikkerhedsarkitektur.

Der er blandt andet oprettet et Security Operations Center (SOC), som er ansvarlig for at overvåge, opdage, analysere og reagere på cybersikkerhedshændelser i realtid.

Databeskyttelsesrådgivere (DPO-funktionen)
DPO-funktionen er en uafhængig funktion, som har en vigtig opgave i forhold til både rådgivning og overvågning af Region Midtjyllands overholdelse af Databeskyttelsesforordningen. DPO-funktionen skal inddrages i regionens overvejelser og beslutninger vedrørende databeskyttelse, herunder også hvordan det sikres, at de databeskyttelsesretlige regler overholdes. DPO-funktionen skal blandt andet inddrages i udarbejdelsen af regionens politikker og retningslinjer omkring databeskyttelse.

Det skal understreges, at DPO-funktionen ikke har ansvaret for Region Midtjyllands overholdelse af de persondataretlige regler. Dataansvaret ligger hos regionens øverste ledelse.

Persondatakonsulenter
Alle større enheder i Region Midtjylland har deres egen lokale persondatakonsulent, som står til rådighed med hjælp og vejledning angående informationssikkerhed. Persondatakonsulenterne har som primær opgave at støtte den lokale enhed i at løse opgaver og udfordringer relateret til informationssikkerhed. Med indgående kendskab til lokal praksis spiller persondatakonsulenterne samtidig en vigtig rolle som sparringspartner og lokal repræsentant i regionens tværgående arbejde med informationssikkerhed.

Linjeledelsen
Det er ledelsens ansvar at sikre, at informationssikkerhedspolitikken overholdes. Ledelsen på alle organisatoriske niveauer har ansvaret for at implementere og støtte informationssikkerhedspolitikken og de vedtagne politikker, retningslinjer og instrukser. Ledelsen skal også bidrage til at øge bevidstheden om sikkerhed og fastholde denne bevidsthed blandt Region Midtjyllands medarbejdere. Desuden er det ledelsens ansvar at vurdere, om der lokalt skal fastsættes et skærpet sikkerhedsniveau ud over den fælles informationssikkerhedspolitik. Alle sikringsforanstaltninger, der besluttes af Informationssikkerhedsudvalget, skal betragtes som basisforanstaltninger, der som udgangspunkt ikke kan fraviges, og de skal overvåges og håndhæves af hele organisationen.

Brud på informationssikkerheden
Hvis en medarbejder opdager trusler mod informationssikkerheden eller et brud på persondatasikkerheden, skal medarbejderen kontakte nærmeste linjeleder, og det skal forsøges at begrænse skaden. Herefter skal det hurtigst muligt rapporteres til henholdsvis Regionssekretariatet ved brud på persondatasikkerheden, og ved it-sikkerhedsmæssige brud skal der rettes henvendelse til 24/7. Medarbejdere, som bevidst bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, kan blive underlagt disciplinære

forholdsregler i overensstemmelse med gældende regler og personalepolitikken i Region Midtjylland.

Ikrafttræden
Det reviderede bilag træder i kraft den 10. april 2024. Den fællesregionale informationssikkerhedspolitik blev vedtaget af Regionsrådet den 24. august 2016.