Regionshuset
Viborg

Regionssekretariatet

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

Dato 04-04-2018

Thomas Madsen Birk
Thomas.Birk@stab.rm.dk

Rikke Stein
Rikke.Stein@stab.rm.dk

1-16-02-13-08

Bilag til fællesregional informationssikkerhedspolitik

Vedlagte bilag skal supplere den fællesregionale informationssikkerhedspolitik, som er vedtaget af Regionsrådet den 24. august 2016. Bilaget skitserer organiseringen af arbejdet med informationssikkerhed og fastsætter sammen med politikken både ansvarsplacering og rammer for dette arbejde i Region Midtjylland.

Organisering
Region Midtjyllands Direktion er øverste ansvarlige for informationssikkerhed. Det er ledelsens ansvar, at informationssikkerhedspolitikken overholdes. Ledelsen på alle organisatoriske niveauer har ansvar for at implementere og understøtte informationssikkerhedspolitikken. De skal samtidig medvirke til at højne sikkerhedsbevidstheden og at fastholde denne blandt Region Midtjyllands medarbejdere. Det er ledelsens ansvar at sikre gennemførelsen og efterlevelsen af informations-sikkerhedshåndbogens retningslinjer om aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger. Samtidig er det også ledelsens ansvar at vurdere, om der lokalt skal være et skærpet sikkerhedsniveau for den fælles informationssikkerhedspolitik.

Den overordnede styring af informationssikkerhedsindsatsen koordineres af Regionssekretariatet. I praksis sker styring i tæt samarbejde med It.

Informationssikkerhedsudvalget
Informationssikkerhedsudvalget udgør det taktiske og strategiske niveau for arbejdet med informationssikkerhed. Udvalget træffer de overordnede administrative beslutninger vedrørende informationssikkerhed i Region Midtjylland.
Udvalget består af den samlede Direktion, én ledelsesrepræsentant fra hhv. sundhedsområdet, psykiatri- og socialområdet og administrationen, it-direktøren, it-sikkerhedschefen (CISO), vicedirektøren for Regionssekretariatet og regionens databeskyttelsesrådgiver (DPO) som tilforordnet.

Styregruppe for informationssikkerhed i Region Midtjylland

Styregruppen er organiseret som en undergruppe til informationssikkerhedsudvalget. Den dækker området informationssikkerhed bredt på det operationelle niveau. Samtidig er projekterne på baggrund af initiativer fra Region Midtjyllands handleplanen for informationssikkerhed forankret her.
Styregruppen skal bidrage til at sikre ledelsens involvering samt synliggøre ledelsens ansvar for informationssikkerhed i organisationen. Styregruppen er en vigtig sparringspartner i forhold til at vurdere forretningens behov for at blive informeret og involveret i de tiltag, der gøres inden for området informationssikkerhed. Gruppen skal være med til at sikre forankringen i hele organisationen.
Udvalget består af én ledelsesrepræsentant fra hhv. sundhedsområdet, psykiatri- og socialområdet og administrationen, it-direktøren, it-sikkerhedschefen, vicedirektøren for Regionssekretariatet og regionens databeskyttelsesrådgiver (DPO) som tilforordnet.

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 Persondataforordningen. DPO funktionen skal inddrages i regionens overvejelser og beslutninger vedrørende databeskyttelse.

DPO funktionen vil i mange tilfælde skulle fungere som brobygger mellem lovgivningen og forretning herunder It. Funktionen vil til en vis grad være en aktiv del af overvejelserne og beslutningerne om, hvordan det sikres, at de databeskyttelsesretlige regler overholdes. DPO funktionen skal blandt andet involveres i f.eks. udarbejdelsen af regionens politikker og retningslinjer indenfor emnet informationssikkerhed. Desuden skal funktionen inddrages i de tilfælde, hvor der skal udarbejdes en konsekvensanalyse blandt andet i forbindelse med udvikling og indkøb af nye applikationer og systemer.

Det skal understreges, at DPO funktionen ikke er ansvarlig for Region Midtjyllands overholdelse af de persondataretlige regler. Dataansvaret ligger hos regionens øverste ledelse. DPO funktionen skal assistere regionen med at sikre intern compliance med forordningen.

Informationssikkerhedsfunktionen
Der er etableret en informationssikkerhedsfunktion i Region Midtjylland.
Informationssikkerhedsfunktionen er en fælles funktion mellem Regionssekretariatet og It. Funktionen er rådgivende og understøttende for Informationssikkerhedsudvalget. Den bidrager til formidling af beslutninger, øvrig information til organisationen samt opfølgning på implementeringen af informationssikkerhedsbeslutninger.
Funktionen rummer tekniske, juridiske og administrative kompetencer. De vigtigste opgaver er at overvåge, at informationssikkerhedspolitikken overholdes og at udarbejde overordnede retningslinjer, instrukser og lignende i overensstemmelse med informationssikkerhedspolitikken.

Informationssikkerhedsfunktionen gennemfører mindst en gang årligt en overordnet risikovurdering, så Direktionen kan holde sig informeret om det aktuelle risikobillede. Informationssikkerhedsfunktionen foretager ligeledes en overordnet risikovurdering ved større forandringer i organisationen. Den øvrige organisation har pligt til at stille oplysninger til rådighed for risikovurderingen efter anmodning fra Informationssikkerhedsfunktionen.

Informationssikkerhedsfunktionens arbejde består desuden af planlægning, implementering og vedligeholdelse, administration, audit og kontrol, information, awarenesstiltag, undervisning og rådgivning om informationssikkerhed i organisationen. Dette arbejde sker i samarbejde med den øvrige organisation.

Lokale Informationssikkerhedskontaktpunkter
Regionens enheder kan vælge at oprette lokale informationssikkerhedskontaktpunkter. De decentrale kontaktpunkter visiterer og besvarer lokale spørgsmål i det omfang, at det er muligt. Enhedernes informationssikkerhedskontaktpunkter kan altid hente rådgivning hos informationssikkerhedsfunktionen. Informationssikkerhedsfunktionen og de lokale informationssikkerhedskontaktpunkter understøtter hinandens arbejde, holder hinanden orienteret og fungerer som hinandens sparringspartnere. De lokale informationssikkerhedskontaktpunkter bidrager til den lokale formidling og overholdelse af de overordnede politikker, retningslinjer og vejledninger.

Anvendelse i praksis
Informationssikkerhedspolitikken definerer et minimumsniveau for informationssikkerhed i Region Midtjylland. Institutioner eller organisatoriske enheder kan efter behov vælge at beslutte et højere sikkerhedsniveau baseret på analyse af risici og karakteren af de informationer, enheden behandler.

Alle sikringsforanstaltninger som besluttes af Informationssikkerhedsudvalget skal betragtes som basisforanstaltninger, der som udgangspunkt ikke kan fraviges og skal håndhæves af informationssikkerhedsfunktionen og informationssikkerhedskontaktpunkterne. Undtagelser og fravigelser skal forelægges Informationssikkerhedsudvalget, der i særlige tilfælde kan give dispensation. Informationssikkerhedsudvalget kan også delegere dispensationsretten, såfremt der er tale om en midlertidig fravigelse.

De retningslinjer, sikkerheds- og kontrolforanstaltninger, der gælder i Region Midtjylland, samles i en sikkerhedshåndbog. Sikkerhedshåndbogen skal indeholde de informationssikkerhedsområder, der er relevante for Region Midtjylland.

Sikkerhedshåndbogen skal være tilgængelig for medarbejderne i Region Midtjylland. Blandt andet skal den kunne findes på Region Midtjyllands intranet.

Brud på informationssikkerheden
Såfremt en medarbejder opdager trusler mod informationssikkerheden eller brud på denne, har den pågældende medarbejder pligt til straks at meddele det til sin nærmeste foresatte, It-sikkerhedsfunktionen eller til Informationssikkerhedsfunktionen.

Medarbejdere, som bevidst eller ubevidst bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, vil kunne blive udsat for disciplinære forholdsregler i overensstemmelse med gældende regler og personalepolitik i Region Midtjylland.

Ikrafttræden
Det reviderede bilag træder i kraft den 3. april 2018. Den fællesregionale informationssikkerhedspolitik er vedtaget i Regionsrådet den 24. august 2016.