**Regionshuset**
Viborg

*Regionssekretariatet*
Skottenborg 26
Postboks 21
DK-8800 Viborg
Tel. +45 8728 5000
kontakt@rm.dk
www.rm.dk

# Informationssikkerhedspolitik for Region Midtjylland

Dato 17-10-2011
Sagsbehandler Lise Tjerrild
Lise.Tjerrild@stab.rm.dk
Tel. +45 7841 0250
Sagsnr. 1-16-02-13-08



## 1. Indledning

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden i Region Midtjylland, og er vedtaget af Regionsrådet.

Politikken er udarbejdet, så den bedst muligt understøtter Region Midtjyllands værdigrundlag og opgaveportefølje samtidig med, at gældende lovgivning overholdes. Informationssikkerhedspolitikken skal udmøntes og håndhæves i overensstemmelse med Region Midtjyllands ledelses- og styringsgrundlag.

Som et led i den overordnede sikkerhedsstyring tager Informationssikkerhedsudvalget på grundlag af den løbende overvågning og rapportering informationssikkerhedspolitikken op til revurdering mindst én gang om året.

Nærværende informationssikkerhedspolitik er udarbejdet med afsæt i anbefalingerne fra den nationalt anbefalede standard for informationssikkerhed ISO27001, som staten har valgt at overgå til. Region Midtjylland har ligesom staten tidligere baseret sig på DS484:2005, men med statens ændrede anbefaling har Region Midtjylland i 2011 ligeledes valgt at skifte til ISO27001.

ISO 27001 er en del af en serie informationssikkerhedsstandarder, der er indbyrdes sammenhængende. Region Midtjylland vil benytte sig af de øvrige standarder i serien eller dele heraf i det omfang, det findes hensigtsmæssigt i den konkrete situation.

## 2. Formål

Information og informationssystemer er afgørende for Region Midtjyllands opgavevaretagelse, og informationssikkerheden har derfor vital betydning for Region Midtjyllands troværdighed og funktionsdygtighed. Som offentlig myndighed har Region Midtjylland en særlig forpligtelse til at sikre, at fortrolige informationer ikke kompromitteres,

samtidig med at regionen tilstræber stor åbenhed overfor offentligheden.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af Region Midtjyllands informationer og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed[1], integritet[2] og tilgængelighed[3]. En klar politik for informationssikkerhed er forudsætningen for, at Region Midtjylland kan vise åbenhed overfor omgivelserne uden at kompromittere sikkerheden.

Derfor har Regionsrådet besluttet sig for et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed, offentlighedens interesser samt overholder lovkrav og indgåede aftaler.



Direktionen i Region Midtjylland vil oplyse medarbejderne om ansvarsforhold i relation til virksomhedens informationer og informationssystemer. Samtidig vil Direktionen arbejde for en kultur, hvor ansvarlighed i forhold til informationsbehandling falder naturligt for alle medarbejdere. Det indebærer blandt andet, at medarbejderne er opmærksomme på at dele viden, skabe information og sikre, at information er tilgængelig uden at dette kompromitterer fortrolige oplysninger.

Hensigten med sikkerhedspolitikken er endvidere at alle, som har en relation til Region Midtjylland, er bekendt med, at anvendelse af informationer og informationssystemer følger nedskrevne standarder og retningslinjer. Man kan derfor trygt afgive information til Region Midtjylland, og som samarbejdspartner er man bekendt med, hvordan man skal behandle information, der modtages i forbindelse med samarbejdet med Region Midtjylland.

På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses, og retablering af informationer kan sikres.

**3. Omfang**

Politikken omfatter alle informationer, som er i Region Midtjyllands varetægt. Det gælder såvel information, der tilhører Region Midtjylland, som information, der ikke tilhører Region Midtjylland, men som Region Midtjylland har ansvaret for. Eksempler på dette kan være data om borgere og patienter; data om personale; data om finansielle

[1] Fortrolighed vil sige, at følsom information ikke kommer uvedkommende i hænde.
[2] Integritet vil sige, at data er korrekte og dermed ikke bliver ændret utilsigtet.
[3] Tilgængelighed betyder, at data kan tilgås af de personer og systemer, der har behov for det, når de har behov for det.

forhold; data, som bidrager til administrationen af Region Midtjylland, samt øvrige informationer, som er overladt Region Midtjylland af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information til internt brug.

Denne politik omfatter al information i Region Midtjyllands varetægt, uanset hvilken form de opbevares og formidles på.

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



Informationssikkerhedspolitikken gælder for alle medarbejdere uden undtagelse såvel fastansatte og personer, som midlertidigt arbejder for Region Midtjylland, uanset om disse modtager vederlag herfor. Disse personer betegnes i det følgende "medarbejderne".

Eksterne leverandører, der varetager opgaver for Region Midtjylland, skal ligeledes leve op til Region Midtjyllands informationssikkerhedspolitik, hvis de har adgang til data, som tilhører Region Midtjylland, eller som Region Midtjylland er ansvarlig for behandlingen af. Når der indgås aftaler med eksterne leverandører, skal det derfor i samarbejde med leverandøren sikres, at Region Midtjyllands sikkerhedsniveau ikke kompromitteres.

Endelig gælder informationssikkerhedspolitikken for andre personer, der gives en særlig adgang til Region Midtjyllands informationer, der overstiger det, offentligheden normalt har adgang til[4].

**4. Organisering**

Der er etableret en informationssikkerhedsfunktion i Region Midtjylland. Informationssikkerhedsfunktionens vigtigste opgaver er at overvåge, at informationssikkerhedspolitikken overholdes og at udarbejde overordnede retningslinjer i overensstemmelse med informationssikkerhedspolitikken.

Informationssikkerhedsfunktionens arbejde skal ske i samarbejde med den øvrige organisation.

Der er nedsat et informationssikkerhedsudvalg bestående af den samlede Direktion, én ledelsesrepræsentant fra hhv. sundhedsområdet, psykiatri- og socialområdet og administrationen, It-chefen og

[4] Det kan fx være i forbindelse med forskningsprojekter, revision, politikeres adgang til information mv.

Sekretariatschefen. Informationssikkerhedsudvalget udgør det taktiske og strategiske niveau for arbejdet med informationssikkerhed. Udvalget træffer de overordnede beslutninger vedrørende informationssikkerhed i Region Midtjylland.

Ledelsen på alle organisatoriske niveauer har ansvar for at implementere og understøtte informationssikkerhedspolitikken og skal medvirke til at højne sikkerhedsbevidstheden og at fastholde denne blandt Region Midtjyllands medarbejdere. Det er således ledelsens ansvar, at informationssikkerhedspolitikken overholdes. Det er ledelsens ansvar at vurdere, om der lokalt skal være et skærpet sikkerhedsniveau ift. den fælles informationssikkerhedspolitik.



Den overordnede styring af informationssikkerhedsindsatsen koordineres af Regionssekretariatet. I praksis sker styring i tæt samarbejde med It. Det er ledelsens ansvar, at det løbende sikres, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i sikkerhedshåndbogen, gennemføres og efterleves.

**5. Sikkerhedsniveau**

Region Midtjyllands tilstræber en høj grad af åbenhed overfor offentligheden. Informationssikkerhedspolitikken og de konkrete retningslinjer skal derfor give vide rammer for at anvende og offentliggøre informationer i forskellige sammenhænge. Dette skal ske under hensyntagen til, at personfølsomme og andre fortrolige informationer beskyttes i henhold til den til enhver tid gældende lovgivning og borgere og virksomheders berettigede forventninger, samt at informationernes integritet og tilgængelighed bevares.

Region Midtjylland fastlægger på baggrund af en konkret risikovurdering[5] et sikkerhedsniveau som svarer til karakteren af de forskellige typer af informationer, der er i regionens varetægt.

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.

Regionsrådet har besluttet, at Region Midtjylland i videst muligt omfang vil leve op til den internationale standard ISO27000. Det betyder, at arbejdet med informationssikkerhedspolitikken, herunder ud-

[5] Risikovurdering i relation til informationssikkerhed er en formaliseret proces for identifikation, prioritering og styring af risici til et acceptabelt niveau i organisationen.

arbejdelse af informationssikkerhedsstrategier og konkrete retningslinjer, baserer sig på denne standard.

Den konkrete udmøntning af standarden skal være beskrevet i en sikkerhedshåndbog.

Sikringsforanstaltninger, der er besluttet af Informationssikkerhedsudvalget, skal betragtes som basisforanstaltninger, der som udgangspunkt ikke kan fraviges. Konkrete ønsker om fravigelse skal forelægges Informationssikkerhedsudvalget, der i særlige tilfælde kan give dispensation. Informationssikkerhedsudvalget kan delegere dispensationsretten.



**6. Sikkerhedsbevidsthed**

Informationssikkerhed vedrører regionens samlede informationsstrøm, og gennemførelse af en informationssikkerhedspolitik kræver en aktiv indsats fra medarbejderne. Alle medarbejdere har et ansvar for at bidrage til at sikre, at Region Midtjyllands informationer ikke kommer uvedkommende i hænde, og at informationer er korrekte og tilgængelige. Det er ledelsens ansvar at sikre, at alle medarbejdere har den fornødne viden om informationssikkerhed, og at der i relevant omfang sker en løbende uddannelse i informationssikkerhed. Tilsvarende er medarbejderne forpligtede til at gøre sig bekendt med den information vedrørende informationssikkerhed, der stilles til rådighed.

Som brugere af Region Midtjyllands informationer skal alle medarbejdere følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende de informationer, der er i Region Midtjyllands varetægt, i forbindelse med det arbejde, de udfører i virksomheden, og i overensstemmelse med informationssikkerhedspolitikken.

Det er desuden vigtigt, at informationssikkerhed indgår som en naturlig del af overvejelserne for alle forretningsgange, driftsopgaver og projekter.

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

## 8. Anvendelse i praksis

De retningslinjer samt sikkerheds- og kontrolforanstaltninger, der gælder i Region Midtjylland, samles i en sikkerhedshåndbog.

Sikkerhedshåndbogen skal indeholde de informationssikkerheds-områder, 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.

## 9. Ikrafttræden

Informationssikkerhedspolitikken er vedtaget i Regionsrådet den 18. marts 2009 og træder i kraft den 18. marts 2009.

Informationssikkerhedspolitikken er senest revideret og godkendt af Regionsrådet den xx.xx 2011.