Regionernes styregruppe for informations- og cybersikkerhed KOMMISSORIUM

1: Basisinformation

Identifikation

Titel	Regionernes styregruppe for informationssikkerhed
Dato + version	3. juli 2018 Ver. 1.2
Godkendelse	27. august 2018
Dokumentation	Seneste version af kommissorium: http://midtrum.rm.dk

Ansvarlige

Deltagende regioner	Alle
Styregruppeformand	Carsten Lind
Medlemmer	Styregruppen sammensættes af: • En formand • 4 medlemmer udpeget af de øvrige regioner • 1 medlem fra Danske Regioner/RSI udpeget af Danske Regioner Medlemmerne udpeges på mindst kontorchefniveau, da de skal have mandat til at træffe beslutninger, der tilgodeser såvel egen organisation som de fælles interesser inden for de i kommissoriet angivne rammer. Regionerne udpeger sine respektive medlemmer. Medlemmerne er på nuværende tidspunkt: Formand: Carsten Lind, Vicedirektør, Region Midtjylland Anna Olga Aaskilde Laursen, CISO, Region Hovedstaden Jan Lehmann Pedersen, Informationssikkerhedschef, Region Sjælland Brian Nyborg Halager, Afdelingschef, Region Syddanmark Karin Bruhn Termannsen, Kontorchef, Region Nordjylland Thue Børsen Lebech, Konsulent, Danske Regioner Sekretær er Malene Nyman, AC-fuldmægtig, Region Midtjylland

	Der kan efter behov inddrages andre på styregruppens møder, eksempelvis arbejdsgruppemedlemmer, projektledere, it-specialister og lignende, såfremt der i styregruppen træffes beslutning om dette.
Sekretariat	Region Midtjylland sekretariatsbetjener regionernes styregruppe for informationssikkerhed. Sekretariatet har til opgave at understøtte arbejdet i styregruppen gennem mødeadministration og som bindeled til Danske Regioner og interne og eksterne samarbejdspartnere. Sekretariatet er tovholder på alle henvendelser til og fra styregruppen. Sekretariatet forestår statusrapportering til RSI. Sekretariatet bistår desuden i forhold til vedligeholdelsen af vidensbanken for informationssikkerhed og formidling af styregruppens beslutninger og lignende. Sekretariatet vil blandt andet løfte følgende opgaver: • Sekretariatsbetjening af styregruppen og underliggende mødefora • Koordinering og styring i forhold til styregruppens opgaver • Formidling af samarbejdets leverancer og styregruppens arbejde • Koordinering og tovholder på vedligeholdelse af leverancer • Koordinering i forhold til fællesregionale tiltag og indsatser • Koordinering i forhold til fællesregional opsamling og udmeldinger • Koordinering og udarbejdelse af statusrapporteringer og lignende • Koordinering af styregruppens nedsatte arbejdsgrupper/projektgrupper
Projekt- og arbejdsgrupper	Styregruppen kan efter behov nedsætte arbejdsgrupper/projektgrupper, som kan understøtte styregruppens arbejde. Der vil typisk være tale om faggrupper, som bemandes med faglige eksperter fra de enkelte regioner, der kan hjælpe styregruppen med at løfte opgaveporteføljen. I første omgang forventes følgende arbejdsgrupper nedsat: • It- og cybersikkerhed • Jura og kontraktkrav • Organisation og ledelse • Databeskyttelsesrådgiverfunktionen

2: Arbejdsrammer

Baggrund og formål	Hver eneste dag behandles følsomme personoplysninger af medarbejdere i regionerne, og regionerne er forpligtet til at sikre, at disse fortrolige oplysninger behandles sikkert, korrekt efter lovgivningen og ikke kommer uvedkommende i hænde. Partierne i Folketinget har i februar 2017 indgået en politisk aftale om syv centrale principper for at nå det fælles mål om at skabe bedre sundhed gennem moderne og sikker brug af data. Principperne lægger blandt andet vægt på: • Datasikkerhed – sundhedsdata skal håndteres sikkert, og patienterne skal kunne forvente, at der bliver passet godt på deres helbredsoplysninger. • Lovlighed, fortrolighed, saglighed og proportionalitet – sundhedsdata må kun bruges til saglige formål inden for lovens rammer. Og brugen af personhenførbare data skal begrænses i størst muligt omfang. En central målsætning i den politiske linje er, at regionerne samarbejder og lærer af hinanden. Regionerne skal arbejde proaktivt med at forbedre sikkerhedsniveauet ved systematisk at undersøge risici og finde muligheder for forbedring. Regionerne skal følge op på både den systemmæssige sikkerhed, den fysiske sikkerhed, lov og kontraktkrav samt overholdelse af sikkerhed blandt personale og i processer. Regionerne skal samarbejde med hinanden, relevante interessenter, myndigheder, leverandører og sundhedspersonale for løbende at forbedre sikkerheden. Regionernes styregruppe for informationssikkerhed repræsenterer regionernes interesser indenfor området og understøtter implementering og efterlevelse af dels folketingets syv principper og dels regionernes politiske linje for informationssikkerhed. For at kunne realisere implementeringen af den politiske linje for informationssikkerhed er det vigtigt, at regionerne har en fælles tilgang til området. Styregruppen er etableret med det formål at sikre, at regionerne samarbejder og opretholder et højt fælles niveau af informationssikkerhed, herunder cybersikkerhed, samt overholder gældende lovgivning. Informationssikkerhed dækker bredt over de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet og tilgængelighed. I arbejdet indgår blandt andet organisering af sikkerhedsarbejdet, påvirkning af adfærd, processer for behandling af data, styring af leverandører samt tekniske sikringsforanstaltninger. Cybersikkerhed omfatter beskyttelse imod de sikkerhedsbrud, der opstår som følge af angreb mod data eller systemer via et eksternt net eller system. Arbejdet med cybersikkerhed fokuserer således på sårbarheder ved sammenkoblingen mellem systemer, herunder forbindelser til internettet. Der er ofte tale om komplekse problemstillinger, og regionerne oplever et stort behov for en fælles koordinering og sparring på området. Dels er det med til at

	lette arbejdet med informationssikkerhed i den enkelte region, hvis der er nogle fællesregionale rammer, retningslinjer og skabeloner at tage udgangspunkt i, og dels vil regionerne med et fælles udgangspunkt stå stærkere i forhold til leverandører og eksterne samarbejdspartnere. I forhold til nye tværregionale projekter skal det sikres, at sikkerhed tænkes ind på forkant. Det betyder, at styregruppen skal følge med i regionernes og de fællesoffentlige aktiviteter og bidrage til, at løsninger etableres og anvendes hensigtsmæssigt og i overensstemmelse med de juridiske og sikkerhedsmæssige rammer. Der er i det hidtidige samarbejde om informationssikkerhed udarbejdet en række tværregionale værktøjer, skabeloner og modeller, som den enkelte region kan bruge i sit eget arbejde med informationssikkerhed. Hensigten er, at den fælles tilgang og indsats på området skal være med til at lette den enkelte regions arbejde med at styrke informationssikkerheden og bidrage til den enkelte regions compliance på området. Anvendelsen af leverancerne forudsætter, at disse løbende skal revideres efter behov. Styregruppen for informationssikkerhed vil derfor forestå den løbende opdatering samt vurdere, hvorvidt der er behov for at udarbejde nye fælles retningslinjer og rammer. Styregruppen for informationssikkerhed indgår i RSI-samarbejdet på det taktiske og operationelle niveau jf. RSI-governance modellen. Gruppen refererer til RSI-direktørkredsen og skal overfor denne og Digitaliseringskredsen rådgive og anbefale indsatser og aktiviteter vedr. informationssikkerhed. Styregruppen orienterer sig via Danske Regioner mod de øvrige styregrupper på samme niveau, RITA og SYS, og deltager i sparring og samarbejde, hvor det er relevant. Desuden skal styregruppen bistå og rådgive Danske Regioner i interessevaretagelsen inden for området og inddrages blandt andet som høringspart i problemstillinger initieret af en enkelt region, Danske Regioner eller en tredjepart.
Opgaver	Styregruppen sikrer en fælles koordineret tilgang og indsats i varetagelsen af følgende opgaver: • Koordinere en tværregional indsats i forhold til informationssikkerhed • Facillitere videns- og erfaringsudveksling mellem styregruppemedlemmerne • Bidrage til, at regionerne opbygger og fastholder et fælles højt sikkerhedsniveau • Bidrage til en fællesregional afklaring og forståelse i forhold til konkrete problemstillinger indenfor informationssikkerhed • Bidrage til fællesregional fortolkning og forståelse af gældende lovgivning • Være sparringspartner for Danske Regioner i forhold til informationssikkerhed • Holde opmærksomhed på relevante RSI-projekter og nationale tiltag • Opfølgning på Cybersikkerhedsstrategi for sundhedssektoren • Rådgive RSI Digitaliseringskredsen og anbefale tværregionale indsatser vedr. informationssikkerhed • Sikre en fællesregional sikkerhedsmæssig og juridisk screening af fællesre-

	gionale projekter og systemer • Levere indspil til strategiske og politisk drøftelser på forskellige niveauer, bl.a. regionsrådenes årlige drøftelse af informationssikkerhed • Koordinerer regionernes reaktion på aktuelle henvendelser fra staten o.l. • Koordinere regionernes reaktion på aktuelle sager i pressen • Etablere tværregionale arbejdsgrupper/projektgrupper • Bidrage til fællesregionale databehandleraftaler • Vedligeholde vidensbank • Opfølgning og vedligeholdelse af de fællesregionale rammer og skabeloner • Vedligeholde den fællesregionale informationssikkerhedspolitik • Foretage løbende opfølgning på indsatsen i regionerne
Fremgangsmåde	Styregruppen vil facillitere, at der sker en vidensdeling blandt regionerne gennem dialog og erfaringsudveksling mellem regionerne både generelt og i forhold til konkrete problemstillinger. Styregruppen vil derfor nedsætte tværregionale arbejdsgrupper, som vil bestå af medarbejdere fra regionerne, som arbejder med informationssikkerhed. Styregruppen vil efter behov indgå i dialog og mødefora med eksterne interessenter som Sundhedsdatastyrelsen, Center for Cybersikkerhed, Digitaliseringsstyrelsen og lignende. Styregruppen for informationssikkerhed afholder møder efter en nærmere fastlagt og offentliggjort plan med 10-11 møder årligt. De fleste af disse er to-timers videomøder, som suppleres med enkelte fysiske heldagsmøder. Herudover vil styregruppen foretage koordinering via mail. Dagsordenspunkter kan indsendes til Styregruppen for informationssikkerhed via sekretariatet af ▪ RSI-direktørkredsen ▪ Digitaliseringskredsen ▪ de enkelte regioner ▪ fællesregionale projekter ▪ Danske Regioner ▪ arbejdsgrupper nedsat under styregruppen for informationssikkerhed Dagsordenspunkter kan være til orientering eller beslutning.
Succeskriterier	1. Regionerne efterlever ISO 27001 som ramme for arbejdet med informationssikkerhed 2. Regionerne har en fælles og koordineret tilgang til arbejdet med informationssikkerhed 3. Regionerne anvender fælles koncepter, værktøjer, skabeloner og modeller, der kan lette den enkelte regions arbejde med at styrke informationssikkerheden 4. Øget opmærksomhed på og viden om informationssikkerhed blandt regionernes medarbejdere, ledelse og politikere 5. Øget juridisk compliance i regionerne gennem optimerede arbejdsgange

	og rutiner i forhold til gældende lovgivning
Forudsætninger og afhængigheder	Styregruppens opgaver og beslutninger vil i mange tilfælde forudsætte en lokal forankring hos den enkelte region. Det er derfor afgørende for opfyldelsen af styregruppens formål, at regionerne forpligter sig til at sikre den lokale forankring af gruppens fællesregionale initiativer i deres egne organisationer. Styregruppen vil have snitflader til andre tværregionale fora og projekter. Dette angår primært overholdelse af lovgivning omkring brug af persondata, opstart af nye digitaliseringsinitiativer, hvor informationssikkerhed skal tænkes ind fra start, samt cybersikkerhed. Endvidere har samarbejdet snitflader til alle regionale og nationale projekter, hvor informationssikkerhed indgår. Styregruppen er afhængig af et godt samarbejde med de nedsatte arbejdsgrupper, øvrige RSI-grupper og eksterne samarbejdspartnere.
Afgrænsning	Styregruppen besidder ikke egne ressourcer udover regionernes fem repræsentanter i styregruppen og sekretariatsbetjening fra Region Midtjylland. Styregruppen er derfor som udgangspunkt ikke udførende på større projekter og opgaver, men fungerer gerne som "styregruppe" og/eller sparringspartner for disse. Iværksættelse af større opgaver og projekter besluttes af RSI, og ressourcer til løsningen af opgaver rekvireres af RSI-direktørkredsen via den almindelige governancestruktur.
Risici	Regionernes interne arbejde med informationssikkerhed er organiseret forskelligt. Der tilstræbes derfor løbende en passende balance mellem ønsket om at skabe en fælles standard i regionerne og det faktum, at regionerne er organiseret forskelligt, og at produktet derfor skal kunne tilpasses den enkelte region. Dette skal være med til at forebygge risikoen for, at regionerne fravælger de fællesregionale rammer og skabeloner. Styregruppen for informationssikkerhed og eventuelle arbejdsgrupper består af repræsentanter fra regionerne, som har andre opgaver i hjemregionen. Der er risiko for, at styregruppen pålægges opgaver, som styregruppen ikke har ressourcer til at løse. Arbejdet med rammerne for informationssikkerhed kan være komplekst og vanskeligt at formidle. Denne kompleksitet indebærer en risiko for, at styregruppens arbejde bliver for abstrakt og afkoblet fra regionernes kerneopgave.
Ressourcer	RSI sikrer, at der i hver region internt afsættes ressourcer svarende til mindst 0,25 årsværk til at dække regionens deltagelse i de grundlæggende aktiviteter såsom møder og mailudveksling. Derudover vil arbejdet med de specifikke, fællesregionale initiativer kræve et ressourceforbrug. Denne indsats må dog antages at være tjent ind i form af sparet arbejde internt i hver enkelt region. Det er svært at estimere regionernes ressourceforbrug yderligere, da det typisk vil variere og afhænge af en række ydre omstændigheder som det aktuelle trusselsbillede, lovgivning osv.

	Herudover bevilges Region Midtjylland ressourcer svarende til 1 årsværk for at varetage sekretariatsbetjening for styregruppen. Endelig kan det overvejes at afsætte ressourcer til løbende ekstern konsulentbistand eller lignende.
Økonomi	Ressourcerne til den enkelte regions indsats svarer til mindst 170.000 kr. årligt. Regionerne afholder selv alle udgifter i forbindelse med medlemmernes deltagelse i møder og øvrige arbejde inden for rammen. Regionerne afregner i fællesskab ca. 650.000 kr. årligt til Region Midtjylland for at dække varetagelsen af sekretariatsbetjening for styregruppen. Der kan evt. foretages en revurdering af forbruget i 2. halvår 2018. Økonomi til udarbejdelse af konkrete løsninger mv. bevilges særskilt af RSI.

Appendiks

A1: Dokumenthistorik

Dato og version	Revision	Ansvarlig
25. april 2017 ver. 1.0		Rikke Stein Lene Møller Manøe
27. august 2018 Ver. 1.1	Generel ajourføring og tilføjelser vedr. cyber-sikkerhed	Malene Nyman

A2: Bilag

Nr	Titel	Beskrivelse
…		