Regionshuset
Viborg

Regionssekretariatet

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

Handleplan for informationssikkerhed 2017 i Region Midtjylland - oversigt over initiativer/faser som forventes afsluttet i 2017

Dato 04-07-2017
Rikke Stein
Tel. +4521359030
rikke.stein@rm.dk
1-16-4-63-17

Begrebsforklaring
Handleplanen for 2017 samler opmærksomhedspunkter dels fra Risikovurdering 2015, dels fra arbejdet med RSI pejlemærket om informationssikkerhed og dels fra Risikoprofilanalysen 2015, der blev afrapporteret til Regionsrådet på møde den 25. maj 2016 som en udvidet forvaltningsrevisionsopgave. Derudover er der inddraget opmærksomhedspunkter fra både eksisterende lovgivning samt den nye EU-persondataforordning, som skal bidrage til, at regionen kan blive parat til de nye love og regler i 2018.

I følgende oversigt over de initiativer, som forventes afsluttet i 2017, er der for hvert initiativ angivet, om det er identificeret fra hhv. Risikovurdering 2015, RSI pejlemærket, forvaltningsrevisionsrapporten eller lovgivning ved hjælp af følgende forkortelser:

RV = Risikovurdering 2015/Risikovurdering 2016
FR = Forvaltningsrevision
RSI = RSI pejlemærket
Lov = lovgivninger, EU-persondataforordning m.v.

Initiativer	RV	FR	RSI	Lov
5.1 **Implementering af fællesregional informationssikkerhedspolitik** Formidling af politikken – målrettet ledelsen.			X	
5.2 **Brugervenlig informationssikkerhedshåndbog** Gøre informationssikkerhedshåndbogen mere brugervenlig og lettere tilgængelig for medarbejdere. Opdatere informationssikkerhedshåndbogen i forhold til ISO 27002:13. Udarbejde strategi for publicering og formidling af håndbogen.	X	X		
5.3 **Tilsyn** Udarbejdelse af retningslinjer for tilsyn med overholdelsen af interne retningslinjer. Organisering af opgaven.				X
5.4 **Udarbejdelse af manglende retningslinjer** Fase 1: Overblik over manglende retningslinjer i forhold til driftens behov og ønsker. Procedure for udarbejdelse af retningslinjer.	X	X	X	X
5.5 **Udarbejdelse af persondatapolitik** Fase 1: Udarbejdelse af persondatapolitik med udgangspunkt i tværregionalt samarbejde påbegyndt. Evt. tilretning af den fællesregionale informationssikkerhedspolitik.				X
6.1 **Udbredelse af ISO standarden** Udarbejdelse af ramme for SoA dokument (Statement Of Applicability)	X	X	X	
6.2 **Informationssikkerhed fra start** Opdatering af RMs projektmodeller, således at juridisk, organisatorisk og teknisk vurdering af informationssikkerhed indgår og løses i projektets indledende fase inden det sættes i drift. Dernæst udarbejdelse af tjekliste/guideline, der kan anvendes bredt i forbindelse med alle nyanskaffelser og opstart af nye initiativer. Fase 1: It-projektmodel Fase 2: mindre udviklingsopgaver	X		X	X
6.3 **Ledelsesmæssig bevågenhed** Drøftelse af informationssikkerhed i Regionsrådet én gang årligt.			X	
6.4 **Persondataforordning og DPO** Analyse af nuværende organisering samt DPO funktion og udarbejdelse af beslutningsoplæg. Tilrette intern organisering i forhold til Persondataforordningen. Beskrivelse og oprettelse af DPO funktionen/stillingen.				X
6.5 **Sikkerhedsfunktionalitet og personoplysninger på mobile enheder m.m.** Fase 1: Udarbejdelse af foranalyse med henblik på at en overordnet afklaring af de sikkerhedsmæssige udfordringer og de juridiske rammer i forhold til mobile enheder m.v. Oplysning: awarenesstiltag blandt andet med fokus på hensigtsmæssig adfærd i forhold til mobile enheder.	X	X		X
7.1 **Informationskampagne (awarenes)** Fase 1: Udarbejdelse af strategi for awareness Gennemførelse af awarenesskampagne for hele Region Midtjylland	X	X	X	X

8.2 **Udredning af klassifikationssystem** Fase 1: Analyse/afklaring af eventuelle gevinster ved at indføre klassifikationssystemet. Herunder Afklaring af hvilke typer klassifikationer, Region Midtjylland skal anvende. Udarbejdelse af beslutningsoplæg		X		
8.3 **Kortlægning af personoplysninger** Fase 1: Udarbejdelse af ramme for kortlægning af personoplysninger og dokumentation af datastrømme med henblik på overholdelse af gældende lovgivning og fremadrettet i forhold til Persondataforordningen. Analyse af den organisatoriske forankring af opgaven med at udføre datastrømsanalyse.	X	X	X	X
8.4 **Optimering af metoden for den årlige risikovurdering** Fase 1: Udarbejdelse af ramme for risikovurdering, herunder: - udvælgelseskriterier og udarbejdelse af flow - revidering af vurderingsskalaer - Implementering af risikovurdering på datastrømme - Udarbejdelse af ramme for risikovurdering af Medicoteknisk udstyr.	X	X	X	
9.1 **Udarbejdelse af retningslinjer for brugerrolle styring (adgangsstyring)** Fase 1: Udarbejdelse af retningslinje og kommunikation om retningslinje til systemejere og øvrige relevante – afhængighed i forhold initiativ 9.2		X	X	X
9.4. **Styring af Administratorkonti (privilegerede rettigheder)** Justering og opdatering af retningslinje for styring af privilegerede adgange både i forhold til interne og eksterne administratorer. Afdække mulighed for central styring af adgange til administratorkonti (f.eks. via BSK). Afhængig af løsningsmuligheder vil der skulle fødes et projekt eller en opgave.		x		X
10.2 **Administration af sikkerhedscertifikater** Afdække nuværende håndtering af sikkerhedscertifikater. Udarbejde en overordnet retningslinje for håndtering af sikkerhedscertifikater. Fase 1: Det er sikret, at at certifikater til vitale services ikke udløber. Det sker gennem implementering af en teknisk løsning, som er underlagt de årlige kontroller.		x		X
12.1. **ISO 27002 tænkes ind i it-service processer** (ITIL) Fortsat implementering af service-management processer (ITIL). Styrkelse af proces for ændringsstyring (change management), herunder at risici og konsekvenser ved ændringer og releases afdækkes, hvilket også er beskrevet i ISO 27002. Fase 1: Som udgangspunkt tager der afsæt i 1-2 processer i 2017, hvor ISO 27002 og ITIL tænkes sammen, men planen er, at samtlige processer skal gennemgås i forhold til, hvordan de behandler personoplysninger og hvorvidt de lever op til standarden – men dette vil ske efter en aftalt plan for implementering og som en del af arbejdet med udarbejdelse af nye processer.		x		
12.2 **Videre opbygning af konfigurationsdatabase (CMDB)** Sikring af, at der er udarbejdet proces og kontrol af opdateringer og sikre at data er retvisende. Initiativet er indeholdt i initiativ 8.1: 'Styring af og overblik over systemer og		X		

processer (aktiver)', hvorfor dette initiativ afsluttes.				
12.3 **Virtuelle servere** Fase 1: Dette er i 2017 sikret gennem adskillelse af test, udvikling og produktionsmiljø/drift samt udarbejdelse og implementering af retningslinjer og vejledninger i organisationen. Principper, herunder funktionsadskillelse, adskillelse mellem adgang til det interne/eksterne miljø, adskillelse mellem test,/udvikling, produktion og undervisningsmiljø (hvor det giver mening), og krav til testmiljø er identificeret og implementeret i organisationen. Styring, oprettelse og nedlæggelse af virtuelle servere sikres gennem udarbejdelse og implementering af retningslinjer og vejledninger.		x		
12.4 **Nøglepersonsafhængighed** Fokus på tiltag som minimerer sårbarheden i forhold til nøglepersonsafhængighed både ressourcemæssigt og kompetencemæssigt	x			
12.5 **Back-up procedurer** Vurdering af, om den nuværende politik for tests af backup er tilstrækkelig, eller om man skal indbygge et minimumsniveau af tests af standardpakkerne, herunder systematisk afprøvning af restore. Afklare om der kan være behov for at ændre på nuværende backup procedure – herunder om der f.eks. skal laves en offline kopi.	X	x		
12.6 **Sikkerhedskopi af bærbare** Undersøge om der sker opbevaring af interne informationer på bærbare enheder, som burde sikkerhedskopieres. I fald dette er tilfældet skal der udarbejdes relevant instruks eller vejledning.		x		
12.8 **Opbevaring af driftslogs** Fase 1: Definition og krav til driftlogs klarlagt. Udarbejdelse af anbefalinger og krav til interne og eksterne log/leverandører i forhold til håndtering af de forskellige typer driftslog. Fokus på det, som driftes eksternt, inden der følges op internt, hvilket kan løbe ind i 2018. Udarbejdelse og implementering af retningslinje i organisationen er gennemført for 2017, men eventuel etablering af logningsprodukt vil ske i 2018.	X	X	X	
12.9 **Gæstenet log** Retningslinje for kontrol af gæstenet-log er udarbejdet og publiceret. Første kontrol er gennemført 2. kvartal 2017, og der vil ske kontrol fremadrettet, hvorfor initiativet afsluttes her.		x		
13.3 **Bedre styring af eksterne leverandøradgange.** Fase 1: Etableret overblik over de IP-adresser, som eksterne har adgang til. Procedure er udarbejdet og implementeret i organisationen.		X		X
14.1 **Testprocedurer og testdata** Generisk testprocedure og tilhørende vejledninger er udarbejdet med udganspunkt i de kritiske systemer og infrastrukturdele identificeret i beredskabet. Udvides løbende, når forretningen efterspørger test af forskellige/yderligere systemer.		X	x	

15.1 **Krav til leverandører** Fase 1: Analyse af hvilke krav, der er nødvendige mhp at sikre, at tekniske og juridiske aspekter bliver vurderet og medtaget ifm udbudsprocesser.		X	X	X
15.2 **Databehandleraftaler** Fase 1: Formidling og implementering af revideret databehandleraftale. Løbende opfølgning på manglende aftaler og sikring af, at der indgås aftaler for nye løsninger påbegyndt. Foranalyse ifht udarbejdelse af ramme for kontrol af databehandlere.	X		X	X
15.3 **SLA aftaler** Gennemgang af nuværende SLA aftaler for kritiske systemer, navngivning i ESDH. Revidering af proces for udarbejdelse af SLA. Proces for løbende opfølgning "Life cycle management".	X			
16.1 **Retningslinje for håndtering af sikkerhedsbrud** Fase 1: Udarbejdelse af overordnede retningslinjer for sikkerhedsbrud Analyse af regionens opfyldelse af notifikationspligten efter EU Persondataforordningen, herunder organisering af opgaven.		X	X	X
17.1 **It-beredskabsplan - fortsat** Videre implementering af it-beredskabsplan Per 1. januar 2017 overgik it-beredskabet til It, hvormed beredskabsplanen er implementeret, og initiativet afsluttes.	X	X	X	x
18.1 **Dokumentation af compliance** Fase 1: Udarbejdelse af ramme for årlig vurdering af den juridiske compliance i regionernes kritiske it-systemer.	X	X	X	X
18.2 **Analyse af EU persondataforordningen** Fase 1: Afklaring af forordningens krav og affødte initiativer vedr. følgende: - Accountability – dokumentationskrav – løftes i andet initaitiv - Håndtering af notifikationspligt – løftes i andet initiativ - Privacy by design/by default – løftes i andet initiativ - Krav til databehandlere – løftes i andet initiativ - DPO – løftes i andet initiativ - Persondatapolitik – løftes i andet initiativ				X
18.3 **Etablering af model for konsekvensanalyse (DPIA - Data Protection Impact Assessment)** Fase 1: Analyse af krav til konsekvensanalyse Udarbejdelse af ramme for konsekvensanalyse				X
18.4 **Samtykke** Fase 1: Analyse af forordningens krav og afklaring af eksisterende processer				X
18.5 **Den registreredes rettigheder** Fase 1: Analyse af de forpligtigelser Region Midtjylland har jvf. gældende ret samt den kommende forordning.				X