Informationssikkerhedspolitik

Sundheds- og Ældreministeriet

Version	Dato	Ansvarlig	Kommentarer
1.0	20131215	Pia Jespersen	Godkendt i KLF 20131121
1.1	20151110	Pia Jespersen	Revision af informationssikkerhedspolitik
1.1	20160127	Pia Jespersen	Rettelser fra KLF møde indføjet. Godkendt i KLF20160126
1.2	20170912	Pia Jespersen	Rettelse vedr. årlig godkendelse. Forelagt KIS
1.3	20180406	Susanne Lyngby	Tilpasset til Databeskyttelsesforordningen
1.4	20180418	Pia Jespersen	Tilføjelse vedr. koncernfælles funktioner
2.0	20180423	Pia Jespersen	Godkendt i KLF 20180423

SUNDHEDS- OG ÆLDREMINISTERIET

1. Generelt

Denne informationssikkerhedspolitik er gældende for hele ministerområdet under **Sundheds- og Ældreministeriet.** Informationssikkerhedspolitikken skal til enhver tid understøtte **Sundheds- og Ældreministeriets** værdigrundlag, vision og de strategiske mål, der fastlægges for organisationen.

Ministeriet har ansvaret for en lang række data, der anvendes til behandlingsformål, kvalitetssikring, forskning, produktion, tilsyn, lægemiddelgodkendelse osv. Data anvendes såvel internt i ministeriet og institutionerne og stilles til rådighed for eksterne parter, herunder brugere andre steder i sundhedsvæsenet.

Dette stiller først og fremmest krav om, at data er tilgængelige for de relevante brugere, når og hvor der er behov for det. **Tilgængelighed** til data skal afpasses efter dette behov.

Tilsvarende er der et krav om **dataintegritet**, dvs. at data, der stilles til rådighed skal være korrekte og opdaterede. Det er særligt kritisk hvor data anvendes direkte i patientbehandling, hvor fejl eller manglende opdateringer kan have betydning for førlighed og helbred.

De oplysninger, der indgår i opgaveløsningen i sundhedsvæsenet, er typisk følsomme oplysninger, herunder personoplysninger, og der er derfor krav om høj grad af **fortrolighed**.

Ministeriets dataanvendelse er meget omfattende og kompleks, og der er behov for at fastlægge sikkerhedsniveauet for anvendelsen konkret i den enkelte databehandling i forhold til vurderingen af risici.

2. Formål

Informationssikkerhedspolitikken skal bidrage til at sikre, at de informationer, som ministeriets institutioner er ansvarlige for, ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes eller kommer uvedkommende i hænde. Politikken har til formål

- at fastlægge de overordnede normer for informationssikkerhed i **Sundheds- og Ældreministeriet**
- at angive ansvarsfordeling og styring af informationssikkerhed i **Sundheds- og Ældreministeriet**
- at fastlægge et tidssvarende og tilstrækkeligt højt sikkerhedsmæssigt niveau i de it-løsninger, ministeriets institutioner er ansvarlige for
-
- at skabe rammen for udarbejdelse af retningslinjer og procedurer vedr. informationssikkerhed. Det skal sikres, at der findes de nødvendige vedligeholdelses- og kontrolfunktioner, så informationsbehandlingen kan ske sikkert og i overensstemmelse med den vedtagne politik.

SUNDHEDS-
OG ÆLDREMINISTERIET

3. Gyldighedsområde/Omfang

Informationssikkerhedspolitikken gælder alle institutioner under ministerområdet for **Sundheds- og Ældreministeriet**, hvor informationer behandles, herunder opbevares og anvendes, uanset i hvilken form.

Informationssikkerhedspolitikken omfatter alle brugere – medarbejdere, konsulenter og andre, der midlertidigt eller for en længere periode har adgang til informationer, som **Sundheds- og Ældreministeriet** eller underliggende institutioner er ansvarlige for.

Endvidere gælder politikken for og hos eksterne samarbejdspartnere, der udfører opgaver for **Sundheds- og Ældreministeriet**. Eksterne samarbejdspartnere skal gøres bekendt med og tiltræde relevante dele af Informationssikkerhedspolitikken.

4. Organisation og ansvar

Departementet fører tilsyn med informationssikkerheden inden for ministerområdet. Formålet med departementets tilsyn er løbende at vurdere, om styringen af informationssikkerheden i de underliggende institutioner er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed sikres i overensstemmelse med det regelgrundlag, institutionen er underlagt.

Den enkelte institutions og departementets ledelse har ansvaret for at informationssikkerhedspolitikken implementeres og efterleves inden for hver enkelt institution, herunder udvikling af lokale informationssikkerhedsstrategier og retningslinjer.

Institutioner, der har outsourcet it-driftsopgaver til en leverandør, eller som indgår i et driftsfællesskab har ansvaret for at fastsætte de nødvendige informationssikkerhedsmæssige krav i en aftale med leverandøren eller driftsfællesskabet i overensstemmelse med sikkerhedspolitikken.

Ministerområdets organisering af informationsanvendelsen betyder, at databehandling i vidt omfang foregår på tværs af institutionsgrænser og i samarbejde med enheder/organisationer uden for ministerområdet. Det er særligt vigtigt at være opmærksom på informationssikkerhed i disse relationer.

Der er i Sundhedsdatastyrelsen etableret en sekretariatsfunktion, der skal koordinere informationssikkerhedsarbejdet i hele **Sundheds- og Ældreministeriet**.

Koncernledelsen har til opgave at sikre en tværgående prioritering af økonomi og ressourcer til organisatoriske eller tekniske sikringsforanstaltninger inden for ministeriets område.

SUNDHEDS- OG ÆLDREMINISTERIET

Etablering af informationssikkerhedsudvalg og placering af roller og ansvar i relation til informationssikkerhedsarbejdet, herunder styring af arbejdet med informationssikkerhed, fastlægges for koncernen og for den enkelte institution og beskrives nærmere i henhold til ISO27001, se nedenfor.

5. Målsætninger

Informationssikkerhedsforanstaltninger skal fastlægges ud fra en konkret vurdering og prioritering, idet der skal være et rimeligt forhold mellem nødvendigheden af en foranstaltning, dens effektivitet og omkostning, herunder, at foranstaltningerne skal gennemføres med mindst mulig ulempe for den daglige anvendelse af de informationer, **Sundheds- og Ældreministeriet** og underliggende institutioner er ansvarlige for.

Målene for informationssikkerheden på **Sundheds- og Ældreministeriets** område er at:

- **Sundheds- og Ældreministeriet** lever op til gældende lovgivning og standarder
- **Sundheds- og Ældreministeriet** er og fremstår som en organisation med en pålidelig it-service og med en troværdig beskyttelse af de informationer, den er ansvarlig for
- Der er størst mulig åbenhed om mål og midler i informationssikkerhedsarbejdet
- Alle kender deres rolle og ansvar
- Ingen uvedkommende kan få adgang til informationer eller informationssystemer, der kan anvendes til at skade borgere, patienter, virksomheder, medarbejdere eller **Sundheds- og Ældreministeriet** selv
- Beskytte fysiske personers rettigheder i forbindelse med behandling af personoplysninger ved at sikre, at de behandles på en lovlig, rimelig og gennemsigtig måde
- Personoplysninger indsamles til udtrykkeligt angivne og legitime formål, og ikke viderebehandles på en måde, der er uforenelig med disse formål
- Sikre dataminimering, så personoplysninger er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt for at opfylde angive formål
- Personoplysninger behandlet inden for ministeriets område er korrekte
- Sikre at personoplysninger anonymiseres eller slettes, når de ikke længere er nødvendige til de formål, hvortil de pågældende personoplysninger behandles
- Etablere passende tekniske og organisatoriske foranstaltninger, der sikrer tilstrækkelig sikkerhed i ministeriets databehandling
- Informationssikkerheden er lokalt forankret og indgår som en naturlig del i det daglige arbejde
- Begrænse konsekvenser af eventuelle skader til en for **Sundheds- og Ældreministeriet** kendt og accepteret størrelse samt sikre, at en videreførelse af databehandlingen efter skade kan ske inden for en accepteret økonomisk ramme og tidshorisont
- Beskytte informationer og systemer ved at opbygge kapacitet til at imødegå og bekæmpe trusler og sårbarheder fra cyberangreb

- Omgåelse eller forsøg på omgåelse af sikkerhedsreglerne opdages og kan tilbageføres til den eller de ansvarlige personer
- Sikre dokumentation for, at organisationen til enhver tid efterlever de opsatte mål

6. Retningslinjer for informationssikkerhed

Beskyttelsen af de informationer, **Sundheds- og Ældreministeriet** er ansvarlig for, skal afstemmes efter risiko, væsentlighed og økonomi samt overholde gældende lovkrav og indgåede aftaler.

Informationssikkerhedspolitikken er baseret på ISO/IEC 27001. Som udgangspunkt skal sikkerhedsniveauet svare til de sikringsforanstaltninger, der er beskrevet her. Hvis sikkerhedsniveauet afviger herfra, skal der foreligge en begrundelse herfor.

Informationssikkerhedspolitikken uddybes i specifikke retningslinjer og forretningsgange, der dækker hovedområderne inden for ISO/IEC 27001:

- Sikkerhedspolitik
- Organisering af informationssikkerhed
- Risikostyring
- Styring af aktiver
- Styring af informationssikkerhed
- Medarbejdersikkerhed
- Fysisk og miljømæssig sikkerhed
- Styring af kommunikation og drift
- Leverandørstyring
- Styring af informationssikkerhedshændelser
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af it-systemer
- It-beredskabsstyring
- Overensstemmelse med lovbestemte krav

Derudover formuleres der retningslinjer og forretningsgange på baggrund af databeskyttelseslovgivningen samt krav og anbefalinger fra Digitaliseringsstyrelsen og Center for Cybersikkerhed, hvor dette er relevant.

Da der inden for ministerområdet er institutioner af forskellig størrelse og varierende kompleksitet og omfang af it-anvendelse, kan der være områder af de ovenfor nævnte, som ikke er relevante for alle institutioner. Ved udarbejdelse af retningslinjer m.v. tages der højde for dette.

SUNDHEDS- OG ÆLDREMINISTERIET

6.1. Risikostyring

Der foretages regelmæssigt en overordnet risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Ligeledes foretages der en risikovurdering ved større forandringer i organisation, arbejdsopgaver eller teknologi. Risikovurderingen er ledelsens beslutningsgrundlag for implementering af nødvendige sikringsforanstaltninger.

I forbindelse med fx ibrugtagning af ny teknologi eller større forandringer i eksisterende teknologi, skal det vurderes, om der skal foretages en konsekvensanalyse. Hvis en behandling af personoplysninger sandsynligvis vil indebære en høj risiko for, at den registrerede får krænket sine rettigheder, foretages der en konsekvensanalyse forud for behandlingen, hvor databeskyttelsesrådgiveren konsulteres.

Hvis konsekvensanalysen viser, at behandlingen vil føre til en høj risiko, som ikke kan begrænses ved at indføre passende foranstaltninger, foretages en forudgående høring af Datatilsynet.

6.2. Leverandørstyring

Ved anvendelse af leverandører eller databehandlere i forbindelse med personoplysninger eller andre fortrolige informationer, skal der ved indgåelse af kontrakter eller leverandøraftaler sikres, at der etableres tilstrækkelige organisatoriske og tekniske sikkerhedsforanstaltninger, og der skal sikres løbende kontrol af sikkerheden ved leverandøren gennem ekstern revision, opfølgning på eventuelle observationer og tilsynsbesøg.

I det omfang, at koncernfælles funktioner fungerer som databehandlere for flere institutioner inden for Sundheds- og Ældreministeriet, skal det sikres, at den løbende kontrol og opfølgning på sikkerheden koordineres mellem de institutioner, der anvender databehandleren.

6.3. Styring af informationssikkerhedshændelser

Hvis en medarbejder opdager brud eller muligt brud på informationssikkerheden, skal det meddeles til den lokale informationssikkerhedsorganisation.

Ved brud på persondatasikkerheden skal Datatilsynet informeres uden unødig forsinkelse og senest 72 timer efter, at sikkerhedsbristen er opdaget, medmindre det er usandsynligt, at bruddet indebærer risiko for fysiske personers rettigheder.

Hvis et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for den registreredes rettigheder, skal den registrerede underrettes. Dette skal ske uden unødig forsinkelse, og underretningen afhænger ikke af tidspunktet for, hvornår der sker anmeldelse til Datatilsynet.

Medarbejdere, som overtræder informationssikkerhedspolitikken eller deraf afledte retningslinjer, er underlagt de sædvanlige personaleretlige disciplinære sanktioner.

Overtrædelser af straffeloven meldes som udgangspunkt til politiet.

SUNDHEDS- OG ÆLDREMINISTERIET

6.4. It-beredskabsstyring

Sundhedsdatastyrelsen har ansvaret for, at der som en del af retningslinjerne foreligger en it-beredskabsplan for håndtering af større informationssikkerhedsmæssige hændelser og tekniske uheld, og at alle relevante personer i organisationen og hos samarbejdspartnere er bekendt med deres pligter og opgaver i forbindelse med sådanne hændelser.

It-beredskabsplanen skal sikre, at skader begrænses mest muligt og at driften i vides muligt omfang kan opretholdes og genoprettes. For forretningskritiske systemer skal der tages stilling til, hvor hurtigt, der skal etableres nøddrift. Der skal foreligge forretningsmæssige nødprocedurer for alle kritiske forretningsområder.

Alle styrelser er part i den koncernfælles it-beredskabsplan. Lægemiddelstyrelsen har endvidere ansvaret for en it-beredskabsplan omfattende it-systemer og -infrastruktur, som ikke indgår i kundeaftalen med Sundhedsdatastyrelsen.

6.5. Informationssikkerhedsbevidsthed

Som dataansvarlige myndigheder er det institutionerne under Sundheds- og Ældreministeriets ansvar at tilse, at medarbejdere og øvrige brugere bliver informeret om, hvilket ansvar der påhviler dem, når de behandler informationer, som ministeriet er ansvarlig for.

Medarbejdere og øvrige brugere af disse informationer skal følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf.

7. Opfølgning og revision

Informationssikkerhedspolitikken skal revideres ved større ændringer eller som minimum hvert år og godkendes af koncernledelsen.

Hver institution og departementet rapporterer til koncernledelsen en gang om året eller efter behov jf. de gældende aftaler i Departementets tilsynskoncept for ministerområdet.

Godkendt i koncernledelsesforum 23.04.2018