

Region Hovedstaden
Informationssikkerhed

Informationssikkerhedspolitik



REGION

Formål

Gyldighedsområde/omfang

Målsætninger

Sikkerhedsniveau

Organisation

Sikkerhedsbevidsthed

Brud på informationssikkerheden

Gennemførelse, opfølgning og revision

Informationssikkerhedshåndbog

Status for ændringer

Version	Dato	Navn	Bemærkning
1.0	24-04-2007		Vedtaget i Regionsrådet

1	Formål	3
2	Gyldighedsområde/omfang	4
3	Målsætninger	4
4	Sikkerhedsniveau	4
5	Organisation	5
6	Sikkerhedsbevidsthed	6
7	Brud på informationssikkerheden	6
8	Gennemførelse, opfølgning og revision	7
9	Informationssikkerhedshåndbog	7

Informationssikkerhedspolitik for Region Hovedstaden

Informationssikkerhedspolitikken skal til enhver tid understøtte Region Hovedstadens værdigrundlag, vision og de strategiske mål, der fastlægges i regionens strategier.

Region Hovedstaden er med sine godt 40.000 medarbejdere en af Danmarks største arbejdspladser. Med bl.a. den elektroniske patientjournal og øget digitalisering af administrative procedurer, bliver det helt essentielt for kvalitet og service, at der er adgang til korrekte og tidstro informationer, når man skal løse opgaver.

De informationer, som indgår i opgaveløsningen, er for en stor dels vedkommende kendetegnet ved, at der er krav om høj grad af fortrolighed (de personfølsomme data). De skal være tilgængelige døgnet rundt, og de må under ingen omstændigheder forvanskes eller mistes.

Ovenstående stiller store krav til sikkerheden i udvikling, implementering og drift af it-løsninger og til medarbejdernes kendskab til og overholdelse af sikkerhedsbestemmelser og -procedurer i forbindelse med informationsbehandlingen.

1 Formål

Informationssikkerhedspolitikken for Region Hovedstaden fastlægger det overordnede ansvar, krav og rammer for at beskytte regionens informationer – både papirbaserede og elektroniske. I særlig grad skal man sikre kritiske og følsomme informationer, så de bevarer deres fortrolighed, integritet og tilgængelighed.

Informationsbehandling med anvendelse af manuelle og it-baserede informationssystemer er nødvendig, for at Region Hovedstaden kan leve op til sine forpligtelser som offentlig myndighed og fremstå som en effektiv, pålidelig og troværdig organisation.

Borgere, virksomheder, samarbejdspartner og andre interessenter har krav på, at der er etableret procedurer i forbindelse med informationsbehandling, som sikrer, at den nødvendige grad af fortrolighed, tilgængelighed og integritet bevares.

Informationssikkerhed skal derfor være en integreret del af den ydelse, Region Hovedstaden leverer til borgere, virksomheder, samarbejdspartner m.fl., lige som det skal være en integreret del af det daglige arbejde for medarbejderne og andre brugere.

Informationssikkerhedspolitikken er rammen for udarbejdelse af retningslinier og procedurer vedrørende informationssikkerhed. Det skal sikres, at der i regionen etableres de nødvendige indbyggede vedligeholdelses- og kontrolfunktioner, så informationsbehandlingen kan ske sikkert og i overensstemmelse med den vedtagne politik og de tilhørende retningslinjer.

Formålet hermed er at forebygge sikkerhedsproblemer, at begrænse eventuelle skader og at sikre at informationer kan reetableres i fald de fortabes.

2 Gyldighedsområde/omfang

Informationssikkerhedspolitikken gælder alle steder i og udenfor regionen, hvor informationer opbevares, anvendes eller behandles, uanset i hvilken form de anvendes eller formidles.

Informationssikkerhedspolitikken omfatter alle brugere - medarbejdere, forskere, konsulenter, regionsrådsmedlemmer, elever, studerende og andre, der midlertidigt eller for en længere periode har adgang til regionens informationer

Alle personer, der får adgang til informationer, regionen har ansvar for, skal overholde informationssikkerhedspolitikken og de tilknyttede -bestemmelser.

Endvidere gælder informationssikkerhedspolitikken for og hos samarbejdspartnere, der opbevarer, anvender eller behandler papirbaserede eller elektroniske informationer efter aftale med regionen.

3 Målsætninger

Regionens sikkerhedsforanstaltninger skal fastlægges ud fra en konkret vurdering, idet der skal være et rimeligt forhold mellem nødvendigheden af foranstaltningen, dens effektivitet og omkostning, herunder at foranstaltningerne skal gennemføres med mindst mulig ulempe for det daglige arbejde.

Målet for informationssikkerheden i Region Hovedstaden er at:

- regionen fremstår som en organisation med en pålidelig it-service og med en troværdig beskyttelse af sine informationer
- der er størst mulig åbenhed om mål og midler i informationssikkerhedsarbejdet, så alle kender deres egen rolle i sikringen af regionens informationer
- regionen på de informationssikkerhedsmæssige områder lever op til lovgivning og nationale standarder
- ingen uvedkommende kan få adgang til informationer eller informationssystemer, der kan anvendes til skade for borgere, patienter, regionens ansatte, eller regionen selv
- informationssikkerheden er lokalt forankret og indgår som en naturlig del i det daglige arbejde
- begrænse konsekvenserne af eventuelle skader til en for regionen kendt og accepteret størrelse samt sikre, at en videreførelse af databehandlingen efter skade kan ske indenfor en accepteret økonomisk ramme og tidshorisont
- omgåelse eller forsøg på omgåelse af sikkerhedsreglerne opdages og kan tilbageføres til den eller de ansvarlige personer

4 Sikkerhedsniveau

Beskyttelsen af regionens informationer, skal afstemmes efter risiko, væsentlighed og økonomi samt overholde lovkrav og indgående aftaler.

Som udgangspunkt skal sikkerhedsniveauet svare til de basale sikringsforanstaltninger i DS484:2005 Standard for Informationssikkerhed. Hvis sikkerhedsniveauet afviger herfra, skal der foreligge en begrundelse herfor.

Standarden indgår i sikkerhedshåndbogen, se kap. 9, og omfatter følgende hovedområder:

1. Organisering af informationssikkerhed
2. Styring af informationsrelaterede aktiver
3. Medarbejdersikkerhed

4. Fysisk sikkerhed
5. Styring af netværk og drift
6. Adgangsstyring
7. Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer
8. Styring af sikkerhedshændelser
9. Beredskabsstyring
10. Overensstemmelse med lovbestemte og kontraktlige krav

Der gennemføres regelmæssigt en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en risikovurdering ved større forandringer.

Risikovurderingen er således ledelsens beslutningsgrundlag i forbindelse med implementering af nødvendige sikringsforanstaltninger.

Sårbarheden overfor hændelser, der kan påvirke informationer og informationssystemer må ikke være højere, end at der kan opretholdes en forsvarlig driftssituation, der understøtter regionens opgaveløsning.

Samtidig skal sikkerhedsniveauet være tilpasset de informationer, der skal beskyttes og de situationer, hvor informationerne anvendes, så sikringsforanstaltninger indpasses bedst muligt i det daglige arbejde.

For særligt følsomme data, f.eks. følsomme personoplysninger eller fortrolige informationer om en leverandøraftale, skal der være etableret ekstra sikkerhed, som f.eks. adgangskontrol, kryptering o.l. ((jf. dataklassifikation)).

Regelmæssigt eller ved væsentlige ændringer i informationsbehandlingen, foretages der en uafhængig vurdering af, om den daglige praksis afspejler politikken, strategien og retningslinjerne, og om disse overholdes.

Koncerndirektionen har ansvaret for, at der foreligger en it-beredskabsplan for håndtering af større informationssikkerhedsmæssige hændelser og tekniske uheld, og at alle involverede personer i informationssikkerhedsorganisationen og linjeorganisationen er bekendt med deres pligter og opgaver i forbindelse med sådanne hændelser.

Beredskabsplanen skal sikre, at skaden begrænses mest muligt og at driften i videst muligt omfang 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.

5 Organisation

Inden for denne informationssikkerhedspolitik er det koncerndirektionen, der har ansvaret for at udvikle en informationssikkerhedsstrategi, der indeholder sikkerhedsmålsætning og overordnede handlingsplaner på området.

Direktionen forelægger politikken til godkendelse i Regionsrådet.

Koncerndirektionen har ansvaret for udarbejdelse af overordnede sikkerhedsretningslinjer.

Det formelle ansvar for implementering og kontrol med overholdelse af informationssikkerhedspolitikken er placeret i linjeorganisationen.

Til støtte for koncerndirektionen etableres der i Koncern IT en enhed for informationssikkerhed. Enheden for informationssikkerhed skal understøtte en harmoniseret implementering og administration af informationssikkerhedspolitikken i hele regionen.

Roller og ansvar i relation til informationssikkerhed, herunder styringen af informationssikkerhedsarbejdet, fastlægges i sikkerhedshåndbogens kapitel vedr. informationssikkerhedsorganisation.

6 Sikkerhedsbevidsthed

Som brugere af regionens informationer skal alle medarbejdere følge informationssikkerheds-politikken og de retningslinjer, der er afledt heraf.

Medarbejdere må kun anvende informationer, som regionen har ansvaret for, i overensstemmelse med de arbejdsopgaver de udfører, og informationerne skal beskyttes i overensstemmelse med deres følsomhed og væsentlighed.

Bevidstheden om sikker anvendelse af regionens informationer gælder også alle andre brugere som forskere, konsulenter, regionsrådsmedlemmer, elever, studerende og andre, der får adgang til regionens informationer. Det er direktionens ansvar at sikre, at alle brugere er bekendt med de retningslinjer, der er gældende for informationer inden for de enkelte forretningsprocesser.

Det er ledelsens opgave at uddanne medarbejderne i informationssikkerhed, samt at oplyse medarbejderne om ansvarlighed i relation til regionens informationer og informationssystemer.

7 Brud på informationssikkerheden

Hvis en medarbejder opdager brud eller mulige brud på informationssikkerheden, skal det meddeles til den nærmeste leder, der videreformidler dette til informationssikkerhedsorganisationen

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

Lovovertrædelser meldes til politiet.

8 Gennemførelse, opfølgning og revision

På baggrund af den overordnede politik udarbejdes der uddybende retningslinjer for håndtering af informationssikkerhed.

Senest 6 måneder efter vedtagelsen af den overordnede politik foreligger 1. version af retningslinjerne vedr. organisering af informationssikkerhed, medarbejdersikkerhed, fysisk sikkerhed og adgangsstyring (jf. oversigten over hovedområder i DS484 i kap. 4).

For øvrige hovedområder foreligger 1. version af retningslinjerne senest 12 måneder efter vedtagelsen.

Implementeringen af retningslinjerne i organisationen gennemføres inden for 6 måneder efter koncerndirektionens godkendelse.

Hvis der er forhold, der gør, at det ikke er muligt at implementere retningslinjerne fuldt ud, kan virksomheds- og stabsdirektører give dispensation fra retningslinjerne efter rådgivning fra Enheden for informationssikkerhed. Dispensationer indberettes årligt til koncerndirektionen.

Koncerndirektionen er forpligtet til årligt at vurdere, om der skal foretages ændringer i informationssikkerhedspolitikken. Denne vurdering gennemføres første gang primo 2009 og indgår i regnskabsaflæggelsen.

9 Informationssikkerhedshåndbog

Informationssikkerhedspolitikken uddybes i regionens elektroniske sikkerhedshåndbog. Håndbogen udbygges og revideres løbende.

Håndbogen vil bl.a. indeholde kapitler, som omhandler Regionens vejledninger, procedurer og mere detaljerede organisering af informationssikkerhedsarbejdet.

- Informationssikkerhedspolitik og -strategi
- Informationssikkerhedsorganisation
- Sikkerhedsfunktionens opgaver
- Styling af informationssikkerhed
- DS484:2005 Standard for informationssikkerhed

- Retningslinjer for informationssikkerhed (sikkerhedsbestemmelser inden for)
 - Risikovurdering og -håndtering
 - Organisering af informationssikkerhed
 - Styling af informationsrelaterede aktiver
 - Medarbejdersikkerhed
 - Fysisk sikkerhed
 - Styling af netværk og drift
 - Adgangsstyring
 - Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer
 - Styling af sikkerhedshændelser
 - Beredskabsstyring
 - Overensstemmelse med lovbestemte og kontraktlige krav
- Kommunikationsplan



**Region
Hovedstaden**

For yderligere oplysninger kontakt
Enheden for informationssikkerhed

Pia Jespersen
Tlf.: 45 11 00 29
Mobil: 20 44 20 11

Jørn Knudsen
Tlf.: 45 11 00 30
Mobil: 26 16 38 57

Finn Verner Nielsen
Tlf.: 45 11 00 31
Mobil: 30 91 62 85

E-mail: informationssikkerhed@regionh.dk

Enheden for informationssikkerhed
Koncern IT
Region Hovedstaden
Borgervænget 7
2100 Kbh Ø