Region Hovedstaden
Informationssikkerhed

2015

Ramme for Informationssikkerhed

REGION

Region Hovedstaden CIMT-Informationssikkerhed

Status for ændringer

Version	Dato	Navn	Bemærkning
1.0	24-04-2007		Vedtaget i Regionsrådet
1.1	13-02-2012	IMT-Informationssikkerhed	Tilpasning af terminologi
1.2	15-10-2012	IMT-Informationssikkerhed	Rettelse af telefonnummer og andre små rettelser
2.0	26-01-2015	CIMT-Informationssikkerhed	Opdatering af dokument, herunder tilpasning til ISO 27001/2

Region Hovedstadens ramme for Informationssikkerhed

Region Hovedstadens ramme for informationssikkerhed skal til enhver tid understøtte Region Hovedstadens værdigrundlag, vision og de målsætninger, der fastlægges i regionen, endvidere skal den efterleve den til enhver tid vedtagne politiske linje for Regionernes målsætninger for informationssikkerhed.

Region Hovedstadens ramme for informationssikkerhed er udarbejdet i henhold til ISO 27001 stk. 5.2 hvor der står: "Topledelsen skal fastlægge en informationssikkerhedspolitik". Denne ramme betragtes som Region Hovedstadens Informationssikkerhedspolitik.

Region Hovedstaden er med sine mange medarbejdere en af Danmarks største arbejdspladser.
Med de mange muligheder som den konstant udviklende teknologi giver, er det essentielt for kvalitet og service at sikre, 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.

Det stiller store krav til sikkerheden i udvikling, implementering og drift af it-løsninger og til medarbejdernes kendskab til og overholdelse af sikkerhedsvejledninger og - instrukser i forbindelse med informationsbehandlingen.

1 Formål

Region Hovedstadens ramme for informationssikkerhed skal sikre at der i organisationen etableres, implementeres og vedligeholdes et ledelsessystem for informationssikkerhed, og at dette løbende forbedres, i henhold til den internationale anerkendte standard ISO 27001 for Informationssikkerhed. Et ledelsessystem i denne sammenhæng betyder at informationssikkerhedsarbejdet overordnet struktureres f.eks. i form af årshjul, anvendelse af værktøjer og fastlæggelse af kontroller.

Rammen for informationssikkerhed fastlægger endvidere det overordnede ansvar og de overordnede 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 varetage sine opgaver efter loven og sine forpligtelser som offentlig myndighed.

Borgere, patienter, virksomheder, samarbejdsparter 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, patienter, virksomheder, samarbejdsparter m.fl., lige som det skal være en integreret del af det daglige arbejde for medarbejderne og andre brugere.

Rammen for informationssikkerhed danner rammen for udarbejdelse af vejledninger og instrukser vedrørende informationssikkerhed. De skal sikre, at der i regionen etableres de nødvendige indbyggede vedligeholdelses- og kontrolfunktioner, så informationsbehandlingen kan ske sikkert og i overensstemmelse med den vedtagne overordnede ramme og de tilhørende retningslinjer samt gældende lovgivning.

Tilvejebringelse af kravene til informationssikkerheden sker gennem et begrundet til- eller fravalg af kontrolmålene i Anneks A, ISO 27001.

Formålet hermed er at forebygge informationssikkerhedsproblemer, at begrænse eventuelle skader og at sikre at informationer kan genskabes efter et nedbrud.

2 Gyldighedsområde/omfang

Rammen for informationssikkerhed gælder alle steder i og udenfor regionen, hvor regionens informationer efter aftale med regionen opbevares, anvendes eller behandles, uanset i hvilken form de anvendes eller formidles. Rammen for informationssikkerhed omfatter altså:

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

- samarbejdspartnere, der opbevarer, anvender eller behandler papirbaserede eller elektroniske informationer efter aftale med regionen, uanset om disse er etableret i eller udenfor Danmark.

Alle personer, der via regionen får adgang til informationer, som regionen har ansvar for, skal overholde rammen for informationssikkerhed og de tilknyttede vejledninger og instrukser.

3 Målsætninger

Ledelsen i regionen ønsker at regionens sikkerhedsforanstaltninger fastlægges ud fra en konkret vurdering, og at der er et rimeligt forhold mellem nødvendigheden af foranstaltningen, dens effektivitet og omkostning, herunder at foranstaltningerne skal gennemføres med mindst mulig ulempe for det daglige arbejde.

Ledelsen ønsker 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 forankres og indgår som en naturlig del af det daglige arbejde i alle dele af organisationen
- 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 informationssikkerhedsreglerne opdages og kan tilbageføres til den eller de ansvarlige personer

4 Informationssikkerhedsniveau

Ledelsen ønsker, at beskyttelsen af regionens informationer skal afstemmes efter risiko, væsentlighed og økonomi samt overholde lovkrav og indgåede aftaler.

Ledelsen ønsker, at sikkerhedsniveauet er tilpasset de informationer, der skal beskyttes og de situationer, hvor informationerne anvendes, så sikringsforanstaltninger indpasses bedst muligt i det daglige arbejde. Regionen skal derfor bestræbe sig på at opnå et tilstrækkelig højt sikkerhedsniveau bredt i organisationen.

Regionens sikkerhedsniveau og risikobillede fastlægges gennem en overordnet risikovurdering, som har til formål at:

- Skabe overblik over risikoprofilen
- Identificere de mest kritiske systemer
- Sikre ledelsens involvering i definition af sikkerhedsniveauet
- Skabe bevidsthed om sikkerhed i organisationen
- Udarbejde en handlingsplan for at imødegå kritiske trusler mod systemerne

Den overordnede risikovurdering omfatter regionens mest kritiske informationsaktiver, og skal gennemføres 1 gang om året, eller hvis der sker væsentlige nye eller ændrede it-tiltag.

For øvrige systemer skal der gennemføres risikovurderinger med passende intervaller, dog minimum hvert andet år, ved nyanskaffelser, eller ved større forandringer.
Risikovurderingerne er således ledelsens beslutningsgrundlag i forbindelse med implementering af nødvendige sikringsforanstaltninger.

Ledelsen eller Regionsrådet kan beslutte at der skal foretages en vurdering, audit, revision m.m.af en ekstern revisor, auditor eller lignende.

5 Beredskab

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 beredskabsorganisationen og linjeorganisationen er bekendt med deres pligter og opgaver i forbindelse med sådanne hændelser. Denne opgave er delegeret til Center for It, Medico & Telefoni.

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.

6 Organisation

I henhold til ISO 27001 standarden pkt. 5.2 skal topledelsen fastlægge en informationssikkerhedspolitik.

Koncerndirektionen har ansvaret for at der foreligger en informationssikkerhedspolitik eller et tilsvarende dokument og en Informationssikkerhedsvejledning. Til støtte for Koncerndirektionen er der i Center for It, Medico og Telefoni (CIMT) etableret et informationssikkerhedsteam, der skal støtte en harmoniseret implementering og administration af rammen for informationssikkerhed i hele regionen. Forslag til rammen for informationssikkerhed og vejledning udarbejdes af CIMT.

Koncerndirektionen forelægger rammen for forretningsudvalg og regionsråd til godkendelse De overordnede vejledninger forelægger CIMT til godkendelse i Direktørkredsen (DK).

Ansvaret for implementering og kontrol med overholdelse af rammen for informationssikkerhed med tilhørende vejledninger er placeret i linjeorganisationen.

Roller og ansvar i relation til informationssikkerhed, herunder styringen af informationssikkerhedsarbejdet, fastlægges i Informationssikkerhedsvejledningerne i kapitel 6: Organisering af informationssikkerhed.

7 Informationssikkerhedsbevidsthed

Alle brugere af regionens informationer skal følge rammen for informationssikkerhed og de vejledninger og instrukser, som regionen har fastsat.

Medarbejdere må kun anvende informationer, som regionen har ansvaret for, i overensstemmelse med de arbejdsopgaver de udfører. 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 vejledninger, der er gældende for informationer inden for de enkelte forretningsprocesser.

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

8 Brud på informationssikkerheden

Enhver bruger, der opdager brud eller mulige brud på informationssikkerheden, skal sikre, at dette meddeles til Service Desk og Informationssikkerhedsteamet enten gennem den nærmeste leder, eller direkte til Informationssikkerhedsteamet.

Enhver borger som har mistanke om uberettiget opslag i interne elektroniske journaler og e-journaler, henvises til Patientombuddet, som er klagemyndigheden i Region Hovedstaden.

En overtrædelse af *rammen for informationssikkerhed* eller *deraf afledte vejledninger er underlagt de sædvanlige personaleretlige disciplinære sanktioner, herunder f.eks. at straffelovsovertrædelser anmeldes til politiet.*.

9 Gennemførelse, opfølgning og revision

Linjeledelse, systemejere m.fl. er ansvarlige for, at der udarbejdes de nødvendige instrukser for håndtering af informationssikkerhed, på baggrund af rammen for informationssikkerhed og vejledninger og for, at de efterleves.

Hvis der er forhold, der gør, at det ikke er muligt at implementere vejledninger og instrukser fuldt ud, kan virksomheds- og stabsdirektører give dispensation efter indstilling fra Informationssikkerhedsteamet. Informationssikkerhedsteamet er forpligtet til årligt at vurdere, om der skal foretages ændringer i rammen for informationssikkerhed. Rammen for informationssikkerhed inkl. ændringsvurdering forelægges årligt for regionsrådet til godkendelse.

Informationssikkerhedsteamet har ansvaret for at rapportere systematisk om effekten af ledelsessystemet for informationssikkerhed til den øverste ledelse i Region Hovedstaden.

10 Informationssikkerheds-vejledningerne

Rammen for informationssikkerhed uddybes i regionens Informationssikkerhedsvejledninger (tidligere kaldet informationssikkerhedsretningslinjer), - som udbygges og revideres løbende.

Fremadrettet skal vejledningerne baseres på de kontrolkrav i ISO 27001/2, som ledelsen skal fastsætte gennem et Statement of Applicability (SoA) dokument, hvor der er foretaget en begrundelse af til- og fravalg. I 2015 vil vejledningerne basere sig på de vejledninger der allerede findes.

Vejledningerne indeholder de konkrete krav og procedurer, som regionen har fastsat for informationssikkerhedsarbejdet.

- Hovedområderne er:
    - Organisering af informationssikkerhed
    - Medarbejdersikkerhed
    - Styring af aktiver
    - Adgangsstyring
    - Kryptografi
    - Fysisk sikring og miljøsikring
    - Driftsikkerhed
    - Kommunikationssikkerhed
    - Anskaffelse, udvikling og vedligeholdelse af systemer
    - Leverandørforhold
    - Styring af informationssikkerhedsbrud
    - Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
    - Overensstemmelse

11 Godkendt

Denne ramme for informationssikkerhed er godkendt i Regionsrådet i Region Hovedstaden d.

Næste revision vil finde sted d.

For yderligere information kontakt:
CIMT – Informationssikkerhedsteamet

E-mail: informationssikkerhed@regionh.dk
Telefon: 38649090
Intranet: http://regi-intranet.regionh.dk/menu/It/Informationssikkerhed/

CIMT – Informationssikkerhedsteamet
Borgervænget 7
2100 København Ø