SYKEHUSET I VESTFOLD

Organisering av personvern- og informasjonssikkerhetsarbeidet

Gjelder for: Hele SiV
Dokumenttype: Retningslinje
Sist endret: 13.02.2024

1. HENSIKT

Hensikten med dokumentet er å klargjøre ansvar og oppgaver innen personvern og informasjonssikkerhet som del av Sykehuset i Vestfold HF (SiV) sitt ledelsessystem for informasjonssikkerhet.

2. ANSVAR

Hvem	Ansvar
Administrerende direktør	- er ansvarlig for å sikre all informasjon i virksomheten (informasjonssikkerheten): o virksomhetssensitive data (jf. virksomhetens klassifisering) o personopplysninger (jf. personvernregelverket)
Ledere på alle nivåer	- har ansvar for informasjon om og implementering av dokumentet i egen enhet. - Informasjonen skal gis til alle i enheten uansett arbeidsforhold (faste, midlertidige, studenter, hospitanter etc.)
Alle ansatte uansett arbeidsforhold (ansatte)	- som i kraft av sin stilling har tilgang til virksomhetssensitive data og personopplysninger, er ansvarlig for å etterleve dette dokumentet.

3. FREMGANGSMÅTE

Det systematiske arbeidet med personvern og informasjonssikkerhet i regionen er beskrevet i dokumentet «NO-04 – Organisering av personvern og informasjonssikkerhetsarbeid».

Dokumentet ligger under «Regionalt styrende dokumenter» her:
Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF (helse-sorost.no)

Dokumentet er del av regionens ledelsessystem for informasjonssikkerhet og skal bidra til å sikre etterlevelse av relevant regelverk og de internasjonalt anerkjente standardene for ledelsessystem for informasjonssikkerhet (NS-EN ISO/IEC 27001) og for personvern (NS-EN ISO/IEC 27701) samt Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen).

SiV er forpliktet etter NO-04 til å plassere utøvende og kontrollerende ansvar og oppgaver innen personvern og informasjonssikkerhet. Dette omfatter beskrivelse av hvilken risiko hver rolle er ansvarlig for (risikoeier).

Risikoeiere skal innen sitt ansvarsområde håndtere usikkerhet knyttet til måloppnåelse. Risikoeiere må vurdere og akseptere risikoen for at mål ikke nås, både når det gjelder helseområdet, personvernområdet og etterlevelse av øvrig regelverk. I dette ligger også krav om egnet informasjonssikkerhet. Hva som er høyeste restrisikonivå som den enkelte rolle kan akseptere, er fastsatt i dokumentet NO-05 «Kriterier for vurdering og aksept av risiko innen informasjonssikkerhet». SiV er i prosess med å gjøre lokale tilpasninger i tråd med dokumentet.

Dokumentet ligger under «Regionalt styrende dokumenter» her:
Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF (helse-sorost.no)

Rollene i SiV er beskrevet nedenfor.

All informasjon skal ha en entydig og identifiserbare eier. Det skal være mulig å finne ut hvem som er ansvarlig for at informasjonen er vedlikeholdt, oppdatert og riktig merket (klassifisert).

SiV benytter seg av informasjonssystemer. Med informasjonssystem menes alle IKT-systemer, IKT-tjenester og IKT-komponenter (maskinvare, programvare) og tilknyttet infrastruktur som inngår i systemene – som brukes til innsamling, lagring, behandling, overføring og presentasjon av informasjon (informasjonsbehandling).

3.1 Administrerende direktør

Administrerende direktør

- er dataansvarlig og risikoeier for SiVs samlede måloppnåelse
- har det overordnede ansvar for egnet informasjonssikkerhet og godt personvern
- er ansvarlig for å påse at SiV har et effektivt internkontrollsystem på personvern- og informasjonssikkerhetsområdet, herunder at:
    - internkontrollsystemet er tilpasset risiko, vesentlighet og egenart.
    - det eksisterer overordnede føringer og prinsipper med tilhørende definert myndighet, roller og ansvar knyttet til SiVs vesentlige og risikoutsatte områder, og at dette er dokumentert i policyer
    - systemet er innrettet slik at det bidrar til at SiV når de mål som er fastsatt, gjennom en målrettet og effektiv drift, pålitelig rapportering og overholdelse av lover og regler

3.2 Systemeier

Alle informasjonssystemer i SiV skal ha en systemeier.

Systemeier er risikoeier for at informasjonssystemet har egnet personvern og informasjonssikkerhet.

- Systemeier er ansvarlig for at et informasjonssystem utvikles, forvaltes og driftes og skal
    - inngå i endringsstyringsprosessen hos IKT-leverandør/databehandler og beslutte gjennomføring av endringer for sitt informasjonssystem
    - sørge for at det kan gis nødvendig opplæring for å kunne benytte informasjonssystemet på korrekt måte
    - overvåke risiko forbundet med informasjonsbehandling og forestå risikovurdering ved behov
    - skal vurdere og i forståelse med personvernombudet, godkjenne uttrekk av informasjon i forbindelse med forskning, undervisning og kvalitetssikring, internt og eksternt

- Systemeier skal sørge for at informasjonssystemet har egnet informasjonssikkerhet og skal
    - gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen (pvf) art. 32
    - sørge for at informasjonssystemet har logging, tilgangsstyring og etterfølgende kontroll, i samsvar med regionale prinsipper for tilgang
    - bistå foretaket i kontinuitetsplanlegging for arbeidsprosesser der informasjonssystemet inngår

- Systemeier skal sørge for at informasjonssystemer oppfyller krav iht. pvf, herunder
    - sikre at informasjonen som behandles i informasjonssystemer vedkommende er systemeier for, er relevant og nødvendig for det definerte formålet. Behandling av personopplysninger skal også ha et rettslig grunnlag og tilfredsstille øvrige plikter i personvernforordningen herunder etterlevelse av krav til innebygd personvern og personvern som standardinnstilling, jf. pvf art. 25
    - at det foreligger skriftlige avtaler (databehandleravtale) med IKT-leverandør/databehandler, jf. pvf art. 28 nr. 3
    - etterlevelse av krav til at personvernkonsekvensvurdering (DPIA) gjennomføres (ved sannsynlig høy risiko for de registrerte), jf. pvf art. 35

- Systemeier utpeker systemforvalter(e)

3.3 Systemforvalter

Systemforvalter er utpekt av systemeier og har det operative ansvaret (faglig/teknisk) for et informasjonssystem på vegne av systemeier for å sikre at informasjonssystemet har egnet informasjonssikkerhet.

Systemforvalter rapporterer til systemeier, og er det normale knutepunktet inn mot ulike brukergrupper mht. «Systemforvaltning». Det vil si anskaffelse, forvaltning, drift, videreutvikling og systemadministrasjon av informasjonssystemet.

Systemforvalters oppgaver ivaretas av en person eller fordeles på hhv **lokal faglig systemforvalter** og **lokal teknisk systemforvalter.**

Nærmere informasjon om disse rollene er under utarbeidelse.

3.4 Informasjonssikkerhetsleder (ISL)

ISL skal

- ha rett til å eskalere informasjonssikkerhetsspørsmål i linjen og direkte til administrerende direktør for SiV, eksempelvis ved behov for nye/endrede sikkerhetstiltak eller tvil om hvorvidt en restrisiko er riktig beskrevet og håndtert

- være en ressursperson, pådriver og tilrettelegger for etablering og gjennomføring av SiVs samlede internkontroll innen informasjonssikkerhet. Til rollen hører blant annet å:
    - lage revisjonsplaner og sikre gjennomføring av sikkerhetsrevisjoner i SiV, samt rapportere planer og resultater gjennom SiVs etablerte kanaler for øvrig revisjonsaktivitet
    - vurdere og følge opp på rapporterte avvik og meddele avvik til sykehuset ledelse i samsvar med SiVs etablerte rutiner for avviksbehandling
    - drive opplysningsvirksomhet i foretaket om informasjonssikkerhet
    - utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområdet

  - gi råd og veiledning i arbeidet med risikovurderinger av informasjonssystemer for å sikre et akseptabelt risikonivå
  - delta i regionale fora for informasjonssikkerhet

- støtte virksomhetsledelsen i spørsmål om informasjonssikkerhet, herunder
  - ha ansvar for faglig rapportering til SiVs ledelse innen sitt fagområde
  - forberede ledelsens årlige gjennomgang av bruk av informasjonssystemet

- kunne akseptere lav restrisiko i henhold til akseptkriteriene [1]

3.5 Personvernombud (PVO)

Personvernombudet skal:

- rapportere direkte til administrerende direktør for SiV, jf. pvf art. 38 nr. 3 siste punkt

Personvernombudet skal ha følgende oppgaver:

- informere og gi råd om personvernforpliktelser
- kontrollere overholdelse av personvernforpliktelser (ikke utføre revisjoner)
- bistå i personvernkonsekvensutredninger (ikke utføre utredningen)
- være kontaktpunkt for de registrerte
- samarbeide med og være kontaktpunkt for Datatilsynet, herunder rådføre seg med tilsynet ved behov og være kontaktpunkt ved forhåndsdrøftinger

Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art., omfang, formål og sammenhengen den utføres i.

Ombudet kan også gis andre oppgaver, men SiV må påse at ombudet ikke pålegges oppgaver eller plikter som fører til en interessekonflikt, jf. pvf art. 38 nr. 6.

3.6 Leder

Leder er risikoeier for måloppnåelsen innen sitt ansvarsområde i samsvar med fastsatte rammer [2].

Ansvaret dekker blant annet å ha tilstrekkelig kontroll med informasjonen og egen, ansattes og underleverandørers bruk av informasjonssystemer i utførelse av arbeidsoppgaver.

Leder skal sørge for at det daglige personvern- og informasjonssikkerhetsarbeidet følges opp innen sitt ansvarsområde, herunder å sørge for at

- informasjonsbehandlingen har egnet informasjonssikkerhet, herunder at risiko knyttet til bortfall av IKT-systemer er vurdert
- at ansatte uansett arbeidsforhold som du er leder for, har tilstrekkelig sikkerhetskompetanse og forståelse av hva som er forventet av dem. Kjennskap til sikkerhetsinstruksens innhold er et minimumskrav
- tilgangsstyringen er egnet, herunder at
  - ansatte uansett arbeidsforhold som du er leder for, får tilgang til informasjon ved behov
  - informasjon er tilstrekkelig skjermet for uberettiget innsyn

[1] NO-5 – Kriterier for vurdering og aksept av restrisiko for informasjonssikkerhet

[2] Blant annet Kriterier for vurdering og aksept av risiko for informasjonssikkerhet (NO-5).

    - informasjon er tilstrekkelig beskyttet mot utilsiktet eller uberettiget endring
- uønskede hendelser og informasjonssikkerhetsbrudd følges opp

Ledere på alle nivåer skal minst en gang årlig vurdere status innen eget ansvarsområde, om leder har tilstrekkelig kontroll med personvern- og informasjonssikkerhetsrisikoen på sitt ansvarsområde.

3.7 Alle ansatte uansett arbeidsforhold (ansatte)

Det er et lederansvar å påse at informasjonen som behandles i en enhet, er klassifisert.

Den enkelte ansatte er ansvarlig for å løse arbeidsoppgavene effektivt og bruke informasjon aktivt (medvirkningsplikt). Dette skal skje med egnet informasjonssikkerhet og godt personvern.

I dette ligger

- å følge SiVs sikkerhetsinstruks og andre sikkerhetsbestemmelser
- å ha en forståelse av hva som er forventet av dem (adferd). For medarbeidere som skal ha tilgang til taushetsbelagte opplysninger, skal også grunnlag og hjemmel for oppslag i de taushetsbelagte opplysningene være forstått
- å søke informasjon ved usikkerhet eller tvil
- å rapportere uønskede hendelser, avvik og informasjonssikkerhetsbrudd i henhold til SiVs avviksrutiner

4. GENERELT

5. INTERNE REFERANSER

1.1.11.1.2	Mål og strategi for informasjonssikkerhet
1.1.11.1.4	Informasjonssikkerhetsinstruks
1.1.11.2.9	Informasjonssikkerhet - Risikovurdering ved nye og endrede IKT-behov og databehandlinger

6. EKSTERNE REFERANSER

Ledelsessystemer for informasjonssikkerhet
Personvernforordningen
Regionalt ledelsessystem for informasjonssikkerhet
Normen (Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren)
Regionale bruksvilkår for informasjonssikkerhet
Personopplysningsloven
NS-EN ISO/IEC 27001:2023 5.3 «Roller, ansvar og myndighet i organisasjonen»

7. VEDLEGG