SYKEHUSINNKJØP

Etableringsplan

Internkontroll for informasjonssikkerhet og personvern

Innholdsfortegnelse

Endringslogg:

Versjon:	Dato:	Endret av:	Kommentar:
1.0	25.5.18	André B.	

1 Innledning

Behandling av informasjon er både kjerneaktivitet og en viktig støtteaktivitet i alle virksomheter. Det er en sentral del av alle arbeidsoppgaver. Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheter skal kunne nå sine mål. Det er da viktig at man kan stole på informasjonen, at den er tilgjengelig og at man følger lover og regler. Informasjonssikkerhet handler om å ivareta dette. Vi kaller det å ivareta nødvendig konfidensialitet, integritet og tilgjengelighet på informasjonen som behandles.

Informasjonssikkerhet omfatter både muntlig, papirbasert og digital behandling av informasjon. Det omfatter også alle typer informasjon, ikke bare enkelte typer som for eksempel personopplysninger og regnskapsinformasjon.

God informasjonssikkerhet er kritisk for virksomheten og handler om å sikre informasjon:

- Fra uvedkommende (konfidensialitet)
- Fra å bli endret, utilsiktet eller av uvedkommende (integritet)
- Å være tilgjengelig ved behov (tilgjengelighet)

Etableringsplanen vil gi en oversikt over aktiviteter man planlegger å gjennomføre for å innføre internkontroll for informasjonssikkerhet, som et steg mot innebygd informasjonssikkerhet og personvern i Sykehusinnkjøp HF. Etableringsplanen er basert på DIFI sin veileder for etableringsaktiviteter av internkontroll for informasjonssikkerhet og veileder for informasjonssikkerhet.

2 Formål

Etableringsplanen formål er å identifisere oppgaver som skal løses og hvordan man løser de, for å følge DIFI sin veileder for internkontroll for informasjonssikkerhet. Man vil også legge vekt på å etablere tiltak for grunnleggende krav i ny personvernsforordning.

Det er identifisert følgende suksesskriterier:

1. God kommunikasjon mellom involverte parter og interessenter.
2. Forankring og støtte fra ledelsen.
3. En fast og velformulert visjon og et godt mandat.
4. Planlegging og gjennomføring gis nok tid og ressurser.

Produktene av etableringsaktivitetene i planen skal danne et godt grunnlag for systematiske aktiviteter for internkontroll for informasjonssikkerhet. Systematiske aktiviteter er kjernen i internkontrollen og kvalitetsleder vil få ansvaret for gjennomføring og vedlikehold.

3 Informasjonssikkerhet og personvern

Stabsdirektør er ansvarlig for å oppfylle krav til informasjonssikkerhet og personvern. Tema er underlagt område for IKT og har som målsetning å oppnå innebygd informasjonssikkerhet og personvern.

Innebygd informasjonssikkerhet og personvern er et overordnet prinsipp i arbeidet med informasjonssikkerhet.

DIFI om innebygd informasjonssikkerhet:

- Innarbeidet i virksomhetsstyringen og understøtter virksomhetens mål.
- Innarbeidet i virksomhetens prosesser og prosjekter fra starten av.
- Tatt hensyn til i hele livssyklusen til IKT-løsninger.
- Et tema alle ansatte i offentlig sektor kjenner til og vet hva innebærer for sine arbeidsoppgaver.

Datatilsynet om innebygd personvern:

- Retten til personvern betyr at systemene vi bruker må oppfylle personvernprinsippene og ivaretar de registrertes rettigheter.
- Personvern som standardinnstilling medfører at virksomheten må hensynta personvern i utviklingen, eller bestilling av programvare, og når man inngår avtaler med leverandører og konsulenter.
- Åpenhet for å kunne svare på hva som behandles, av hvem, hvorfor, hvordan, hvor og hvor lenge. Det må sikres legitimitet og effektivitet for den behandlingsansvarlige.
- Forankring hos ledelsen er avgjørende for at virksomheten klarer å overholde personvernet.

4 Etableringsaktiviteter

Her følger en overordnet oversikt over etableringsaktivitetene. Merk at det er både parallelle og sekvensielle aktiviteter.

Aktivitet 1: Analyse og kartlegging

DIFI sin veileder: Man må vite om hvor man er for å vite om status er tilfredsstillende eller om noe bør gjøres. Dersom man er usikker på om omfang og kvalitet i internkontrollarbeidet på informasjonssikkerhetsområdet er godt nok, bør man får gjennomført en analyse av status. Analysen bør gjennomføres av en liten arbeidsgruppe med god innsikt i virksomhetens organisering, aktiviteter og eksisterende internkontroll. Gruppen må normalt snakke med flere interne aktører.
Gjennomføring: IKT-leder vil få ansvaret for å gjennomføre en analyse og kartlegging av virksomheten. Resultatet fra kartleggingen vil inngå i en konfigurasjonsoversikt og bli benyttet som grunnlag for gjennomføring av etableringen. Analyser, kartlegging og klassifisering vil gjennomføres i samsvar med DIFI sine veiledere basert på følgende ISO standarder: 9001, 27000, 27001 og 27002.

Aktivitet 2: Planlegge etablering

DIFI sin veileder: Beslutter virksomhetsledelsen at man skal etablere eller vesentlig forbedre internkontrollen bør de peke ut noen som skal lage og følge opp en plan for arbeidet.
Praktisk gjennomføring: Ansvaret for prosessens planlegging og gjennomføring er lagt til Stabsdirektør, mens den praktiske gjennomføringen er lagt til IKT-sjef i kraft av rollen som fagansvarlig for informasjonssikkerhet. Administrerende direktør orienterer styret etter avtale. Planen for internkontroll for informasjonssikkerhet som man nå leser følger DIFI sin veileder og viser konkrete gjennomføringsmetoder for aktivitetene.

Aktivitet 3: Utforme styrende dokumenter

DIFI sin veileder: Styrende dokumenter er fundamentet i internkontrollen. De klargjør hvem som skal gjøre hva, og gir føringer for arbeidet. De er en forutsetning for at de systematiske aktivitetene i internkontrollen gjennomføres i tilstrekkelig omfang og på riktig måte. Følgende dokumenter vil opprettes: • Overordnede rammer for etableringen av internkontroll for informasjonssikkerhet • Overordnede retningslinjer for internkontroll for informasjonssikkerhet • Roller og ansvar i internkontroll- og sikkerhetsarbeidet • Systematiske aktiviteter • Forstå, vurdere og håndtere operativ risiko • Aktiviteter og ansvar for internkontroll
Praktisk gjennomføring: Følgende dokumenter ble godkjent av styret 12.10.17 og kan erstatte «forstå, vurdere og håndtere operativ risiko» og «Aktiviteter og ansvar for internkontroll»: • Prinsipper for internkontroll • Styringsprinsipper Arbeidet med å utforme styrende dokumenter vil bli gjennomført i samråd mellom kvalitetsleder og fagansvarlig informasjonssikkerhet, med aktuelle roller i sikkerhetsorganisasjonen. Dokumentene blir revidert etter hvert som ulike aktører blir identifisert i virksomheten. Styrende dokumenter godkjennes iht. virksomhetens styringsprinsipper.

Aktivitet 4: Ansvar og roller i sikkerhetsorganisasjonen

DIFI sin veileder: Ansvaret for informasjonssikkerhet og tilhørende internkontrollarbeid bør som hovedregel følge linjen. For å understøtte både virksomhetsleder og linjen, må virksomheten etablere tilstrekkelige fellesfunksjoner, støttefunksjoner og samarbeidsgrupper.

Viktige roller som må tildeles:

- Personvernombud
- Fagansvarlig informasjonssikkerhet

Praktisk gjennomføring:

Fagansvarlig for informasjonssikkerhet og prosjektleder må identifisere hvem det er hensiktsmessig å inkludere i sikkerhetsorganisasjonen. Dette må gjøres for å gjennomføre andre aktiviteter og for å sikre måloppnåelser for internkontroll for informasjonssikkerhet.

Aktivitet 4.1: Identifisering av nøkkelpersoner

DIFI sin veileder:

Virksomhetens ledelse har ansvar for at det finnes ressurser som kan inngå i de systematiske aktivitetene. Det forutsettes kompetanse innen aktuelle fagfeltet og tilstøtende støttekompetanse som pedagogikk. Det er også viktig å påse at den enkelte ansatte har kapasitet til å delta over tid.

Sentralt for systematiske aktiviteter er å identifisere tjenester/informasjonselementer som skal klassifiseres, samt identifisere roller som ikke benyttes i dag, eksempelvis tjenesteansvarlig og systemeier.

Praktisk gjennomføring:

Modelleringen IKT-avdelingen gjennomfører vil identifisere nøkkelpersoner som tjenesteansvarlig og systemeier i virksomheten. De identifiserte nøkkelpersonene vil være nødvendig for gjennomføring av aktiviteter som 7, 9 og 10.

Aktivitet 5: Utforme og gjennomføre grunnopplæring

DIFI sin veileder:

Når overordnede styrende dokumenter er ferdig og godkjent, bør virksomheten har ferdig informasjonsmateriell til internt bruk. Man bør i tillegg spesielt vurdere om og hvordan det eventuelt bør gjennomføres informasjon, opplæring og kulturutvikling for:

- Systemeiere fellessystem
- Felles tiltaksleverandører
- Prosessledere i aktivitetene «Få oversikt og prioritere, gjennomføre risikovurdering og foreslå håndtering av risikoer».
- Alle ansatte.

Det behøver ikke skje med en gang, men legges inn i planen for etablering.

Praktisk gjennomføring:

Læringsmidlene vil være sammensatt av DIFI sitt kursmateriell og vil blant annet bestå av rollespill, nettkurs og diskusjoner med dilemmatrening.

Følgende vil opprettes:

- Informasjonspakker tilpasset organisasjonen.
- Opplæringspakker tilpasset virksomhetens fagområder.
- Forslag til årshjul for videre opplæring.

Læringsmidlene vil tilpasses av ansatte i stab/fellesfunksjoner i samråd med sikkerhetsorganisasjonen og nøkkelpersoner. Dette vil bidra til at stab/fellesfunksjoner blir et kompetansesenter for området for å på best mulig måte kan støtte opp under linjeorganisasjonens arbeid med feltet.

Gjennomføre opplæring:

- Grunnopplæring gjennomføres for stab/fellesfunksjoner.

HR-avdelingen vil få ansvar for at nyansatte gjennomgår opplæringen som en del av on-boardingen, mens ansvaret for den praktiske gjennomføringen vil bli lagt til fagansvarlig for informasjonssikkerhet.

Aktivitet 6: Etablere system for hendelse- og avvikshåndtering

DIFI sin veileder:

Risikoer må identifiseres, vurderes og håndteres både jevnlig og når de inntreffer. En viktig støtte er et hensiktsmessig system for hendelses- og avvikshåndtering. Det vil gi oss en systematikk for håndtering med klare føringer om:

- Hva som skal rapporteres
- Hvem som skal rapportere og når det skal rapporteres
- Hvordan rapporteringen skal skje
- Hvem som skal håndtere hva
- Hvem som skal informeres om hva

Praktisk gjennomføring:

Sikkerhetsorganisasjonen vil opprette prosedyre for hendelser og avvik etter ITIL-rammeverket, og implementere dette i saksbehandlingssystem for IKT. Dette kan kobles på virksomhetens styringssystem når dette er implementert.

Aktivitet 7: Etablere fellessikring og synliggjøre tilleggssikring

DIFI sin veileder:

En virksomhet kan ha et felles grunnleggende sikkerhetsnivå for sentrale områder i virksomheten. Et felles grunnleggende sikkerhetsnivå i en virksomhet kaller vi virksomhetens fellessikring. Fellessikring består av sikkerhetstiltak som bidrar til sikkerheten for mange systemer og arbeidsoppgaver. Det er tiltak som er felles for mange, eller alle, arbeidsoppgaver og systemer i virksomheten.

- Man oppnår en rekke fordeler med å etablere et slikt felles grunnleggende nivå av sikkerhet: felles forståelse av hvilken grunnleggende sikkerhet som er etablert i virksomheten
- trygghet for at informasjonsbehandling har et visst grunnleggende nivå av sikkerhet
- oversikt over sikkerhetstiltak på sentrale områder
- en grunnmur som ekstra sikkerhetstiltak kan bygges på der det er spesielle behov

Praktisk gjennomføring: Sikkerhetsorganisasjonen vil i samråd med identifiserte nøkkelpersoner benytte informasjon fra kartleggingen som grunnlag for å avdekke hvilke tiltak som eksisterer, eller bør eksistere, men som ikke finnes i risikoregisteret. Avdekkede tiltak vil ved prosjektets slutt overleveres kvalitetsleder for videre vedlikehold.

Aktivitet 8: Etablere rammeverk for dokumentasjon

DIFI sin veileder: Dersom internkontrollen skal fungere, må nødvendig informasjon være tilgjengelig for de som har behov for den. Dette sikres best ved at virksomheten har et tydelig rammeverk for internkontroll og virksomhetsstyring.
Praktisk gjennomføring: Sikkerhetsorganisasjonen vil opprette et rammeverk for dokumentasjon som er tilpasset virksomhetens generelle internkontroll og virksomhetsstyring

Aktivitet 9: Identifisere typiske oppgave- og informasjonstyper

DIFI sin veileder: Å få oversikt for å kunne prioritere er en sentral del av arbeidet. Dette er en langvarig prosess som bør sakte og systematisk utvides til flere og flere organisatoriske enheter, med formål å avdekke typiske oppgaver og informasjonstyper virksomheten forvalter.
Praktisk gjennomføring: DIFI har en eksempelsamling man kan benytte frem til virksomheten har en egen samling over typiske oppgave- og informasjonstyper. Identifiserte risikoeiere er ansvarlig for forvaltning av virksomhetens egen samling. Ansvaret er lagt til fagansvarlig for informasjonssikkerhet.

Aktivitet 10: Felles analyse av eksterne krav

DIFI sin veileder: En felles analyse av eksterne krav vil være en støtte for DIFI sin systematiske aktivitet "Analysere eksterne krav" og har som formål å identifisere konkrete krav om sikkerhetstiltak eller typer tiltak regelverket virksomheten må forholde seg til.
Praktisk gjennomføring: Det er allerede gjennomført en analyse av eksterne krav som inngår i virksomhetens generelle internkontroll og en oversikt ble laget november 2017. Risikoeiere (systemeiere) vil benytte det eksisterende registeret og tilføye krav til tiltak som mangler. Ansvaret er lagt til fagansvarlig for informasjonssikkerhet.

Oppsummering av aktivitetene:

Tidsrom	Aktivitet	Beskrivelse/produkt
2017- uke 21 2018	1. Analyse og kartlegging	Baseline.
Uke 16-20	2. Planlegge etablering	Plan er utarbeidet.
Uke 20-26	3. Utforme styrende dokumenter	Arbeidspakke fordelt innen uke 23. Frist for ferdigstillelse er uke 26.
Uke 20-26	4. Ansvar og roller i sikkerhetsorganisasjonen	Roller identifiseres og formaliseres fortløpende, og ansvar blir fordelt.
Uke 20-26	4.1 Identifisere nøkkelpersoner	Man har identifisert tjenester/informasjonselementer og tjenesteansvarlig og systemeiere. Opprettede protokoller må vedlikeholdes videre av kvalitetsleder.
Uke 25-30	5. Utforme og gjennomføre grunnopplæring	Man har et strukturert og tilpasset kurs og informasjonsmateriell som kan benyttes for videre opplæring og informasjonsarbeid.
Uke 27 *Anbefalt milepæl med påfølgende rapportering til ledergruppen i august 2018.*	6. Etablere system for hendelse- og avvikshåndtering	Implementert prosedyre for håndtering av hendelser og avvik som kan tilpasses det planlagte styringssystemet.
Oppdateres etter neste milepæl	7. Etablere fellessikring og synliggjøre tilleggssikring	En oversikt over eksisterende og potensielle tiltak for sikkerhet for alle nivåer og områder.
Oppdateres etter neste milepæl	8. Etablere rammeverk for dokumentasjon	Sikkerhetsorganisasjonen vil opprette et rammeverk for dokumentasjon som er tilpasset virksomhetens generelle internkontroll og virksomhetsstyring.
Oppdateres etter neste milepæl	9. Identifisere typiske oppgave- og informasjonstyper	Virksomheten får en samling eksempler over typiske oppgave- og informasjonstyper.
Oppdateres etter neste milepæl.	10. Felles analyse av eksterne krav	Et oppdatert register over eksterne krav til tiltak.

Veien videre og systematiske aktiviteter:
Når etableringsaktivitetene er gjennomført og ansvar og roller i sikkerhetsorganisasjonen er fordelt, beskrevet og dokumentert, vil prosjektet overleveres kvalitetsleder. Kvalitetsleder vil dermed overta ansvaret for å integrere internkontroll for informasjonssikkerhet som systematiske aktiviteter på linje med den generelle internkontrollen. Man har som et foreløpig mål om å gjennomføre og ferdigstille etableringsaktivitetene innen november 2018. Dette er en foreløpig frist ettersom flere av aktivitetene er avhengig av ansatte fra linjeorganisasjonen for å gjennomføres.

5 Lenker

Aktivitetene er basert på DIFI sin veileder «Etableringsaktiviteter»:
http://internkontroll.infosikkerhet.difi.no/etableringsaktiviteter

Datatilsynet om innebygd personvern:
https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/?id=7728