Sykehusinnkjøp HF

Organisasjonsnummer 916 879 067
Telefon 78 95 07 00
post@sykehusinnkjop.no
Sykehusinnkjøp HF, Postboks 40, 9811 Vadsø

System for informasjonssikkerhet og personvern

Konfidensialitet – Integritet – Tilgjengelighet

Godkjent av:	Administrerende direktør
Gyldig fra:	1. januar 2025
Gjelder for:	Alle ansatte
Dokumenteier:	Informasjonssikkerhetsleder
Versjon:	2.0
Nivå:	2

SYKEHUSINNKJØP

Innholdsfortegnelse

1. Formål 3
2. Omfang 3
2.1. Grunnlag 3
2.2. Sentrale drivere 3
2.3. Forvaltning 3
2.4. Dokumentasjon 4
3. Ansvar 4
4. Relaterte dokumenter 4
5. Versjonshistorikk 5

1. Formål

System for informasjonssikkerhet og personvern er en forutsetning for at Sykehusinnkjøp HF kan håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Videre er Sykehusinnkjøp HF som behandlingsansvarlig, pålagt å ha egnede tiltak, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i samsvar med regelverket. System for informasjonssikkerhet og personvern vil sikre at Sykehusinnkjøp HF klarer å ivareta pliktene etter gjeldende regelverket.

Sykehusinnkjøp HF er et nasjonalt foretak som leverer anskaffelses- og innkjøpsrelaterte tjenester til norske sykehus. De fire regionale helseforetakene eier foretaket og er samtidig våre oppdragsgivere. Foretaket har divisjonskontor i hele landet og hovedkontoret ligger i Vadsø. Sykehusinnkjøp HF skal ha strategisk og operativt ansvar for innkjøp i hele spesialisthelsetjenesten, og være profesjonell, spesialisert og tilgjengelig for brukerne.

God informasjonssikkerhet og personvern er en forutsetning for vellykket digitalisering og styring av risiko i oppgaveutførelse og tjenesteleveranser.

2. Omfang

System for informasjonssikkerhet og personvern gjelder for alle deler av foretaket, hele organisasjonen og all egen virksomhet. Systemet skal sikre at foretakets forvaltning av informasjon og dokumentasjon er i samsvar med gjeldende krav til informasjonssikkerhet ved behandling av forretnings- og personopplysninger, inkludert kodede/avidentifiserte opplysninger.

2.1. Grunnlag

System for informasjonssikkerhet og personvern skal bidra til å sikre etterlevelse av gjeldende lov- og forskriftskrav, ivareta foretakets forpliktelser og ansvar i forholdet til egen organisasjon og andre virksomheter. Det gjøres gjennom å gi overordnede føringer og prinsipper for arbeid med å tydeliggjøre og følge opp roller, ansvar, oppgaver og aktiviteter knyttet til informasjonssikkerhet og personvern.

2.2. Sentrale drivere

System for informasjonssikkerhet og personvern er en forutsetning for en sikker og effektiv behandling av data og personopplysninger. Dette gir forutsigbar kontroll på et sentralt fagområde som foretaket plikter å ivareta. Effekten av en vellykket implementering og kontinuerlig forbedring vil redusere risiko for uønskede hendelser og sikkerhetsbrudd.

2.3. Forvaltning

Forvaltning av dokumentasjon for systemet ivaretas i sikkerhetsrådet, hvor representantene er gitt det faglige ansvaret. Dette omfatter følgende:

- Systematisk revisjon av dokumentene, minimum en gang årlig.
- Ved behov for oppdateringer, tillegg eller andre endringer, meldes dette inn til foretakets informasjonssikkerhetsleder, som tar saken opp i sikkerhetsfaglige råd.
- Behov for oppdateringer og nye dokumenter bearbeides i sikkerhetsfaglig råd. Ved faglig enighet i rådet oppdateres aktuelle dokumenter. Tilsvarende ved behov for nye dokumenter. Endringer skal minimum informeres om i den enkelte leders linje i tillegg til Personvernombudet før endringer trer i kraft.
- Ved større endringer, må beslutning sikres forankring i foretakets ledelse.

2.4. Dokumentasjon

System for informasjonssikkerhet og personvern (dette dokumentet)

- Regelverk for informasjonssikkerhet
- Organisering av informasjonssikkerhetsarbeidet
- Sikkerhetsmål og akseptabel risiko for informasjonssikkerhet
- Strategi for informasjonssikkerhet
- Sikkerhetsinstruks
- Mandat for IKT-utviklingsråd
- Mandat for IKT-sikkerhetsråd
- Prinsipper for behandling av personopplysninger
- Retningslinjer for behandling av personopplysninger

Ovenstående styrende dokumenter skal inngå i foretakets internkontroll, hvor informasjonssikkerhet er eget fagområde som skal omfattes av:

- Revisjon
- Avvikshåndtering
- Ledelsens gjennomgåelse

3. Ansvar

Det er virksomhetens ledelse ved administrerende direktør som er ansvarlig for foretakets informasjonssikkerhet og som formelt er behandlingsansvarlig, jf. personvernforordning artikkel 4, nummer 7 og artikkel 5 nummer 2.

Foretakets administrerende direktør har besluttet å delegere myndighet for oppfølging av informasjonssikkerhet til virksomhetens informasjonssikkerhetsleder. Spørsmål vedrørende personopplysningssikkerheten skal avgjøres i samråd med juridisk avdeling og personvernombudet. jf. Organisering av informasjonssikkerhetsarbeidet.

4. Relaterte dokumenter

Type	Nivå	Tittel	Undertittel
	2	Informasjonssikkerhet og personvern Vedlegg 1	Regelverk for informasjonssikkerhet
	2	Informasjonssikkerhet og personvern Vedlegg 2	Sikkerhetsmål og akseptabel risiko for informasjonssikkerhet
	2	Informasjonssikkerhet og personvern Vedlegg 3	Strategi for informasjonssikkerhet
	2	Informasjonssikkerhet og personvern Vedlegg 4	Organisering av informasjons-sikkerhetsarbeidet
	2	Informasjonssikkerhet og personvern Vedlegg 5	Informasjonssikkerhetsinstruks
	2	Informasjonssikkerhet og personvern Vedlegg 6	Mandat IKT-sikkerhetsråd
	2	Informasjonssikkerhet og personvern Vedlegg 7	Mandat IKT-utviklingsråd
	2	Prinsipper for behandling av personopplysninger	

	2	Retningslinjer for behandling av personopplysninger	

5. Versjonshistorikk

Dato	Versjonsnr	Merknad til versjonen
01.05.2022	1.0	Nytt dokument
17.12.2024	2.0	Dokumentets innhold er lagt over på riktig foretaksmal. Det er gjort nødvendige tilpasninger av dokuments innhold i tråd med føringer gitt i arbeidet med tiltaksplan knyttet til internrevisjon for Informasjonssikkerhet og personvern, Fase 1