HORDALAND FYLKESKOMMUNE

ORGANISASJONSAVDELINGA
Stab - Org avd

Notat

Dato: 08.05.2015
Arkivsak: 2014/12288-8
Saksbehandlar: rangjer

Til:	Fylkesutvalet
Frå:	Fylkesrådmannen

Mål og strategi for informasjonstryggleik 2015-2019

Informasjonshandsaminga i Hordaland fylkeskommune skjer hovudsakleg ved hjelp av informasjonssystem. Bruk av informasjonsteknologi gjer det mogleg og er naudsynt for å løyse fylkeskommunale oppgåver effektivt. Samstundes vil bruk av slik teknologi stille krav til fylkeskommunen om forsvarleg handsaming av opplysningane som vert samla inn.

Informasjonstryggleik er eit samleomgrep knytt til krav til pålitelegheit og tryggleik for informasjon.

Det vedlagte dokumentet er Hordaland fylkeskommunes overordna styrande dokument for informasjonstryggleik. Mål for informasjonstryggleik beskriv kva ein ønskjer å oppnå innanfor informasjonstryggleik, medan tryggleiksstrategien beskriv kva tiltak som skal gjennomførast for å nå måla.

Bakgrunn
Informasjon er i dagens samfunn ein ressurs som må vernast. All informasjon som vert handsama og oppbevart i ein organisasjon kan utsetjast for truslar, og er difor sårbar. Informasjonstryggleik skal være eit middel for å hjelpe organisasjonen med å nå sine mål, samstundes som ein oppfyller lovkrav og opprettheld eit godt image. Dette gjeld uansett korleis informasjonen vert lagra (t.d. elektronisk eller på papir), og korleis den vert flytta.

Hordaland fylkeskommune handsamar personopplysningar av ulik karakter om tilsette, elevar og lærlingar, pasientar i tannhelsetenesta, brukarar av ulike tilskotsordningar, kundar av samferdselstenester og samhandlingspartnarar i offentleg og privat sektor. I fylkeskommunen er det ei mengd informasjonssystem som inneheld personopplysningar.

Dei fleste knyt omgrepet informasjonstryggleik til ein av to: it-tryggleik eller personopplysningar. Informasjonstryggleik er likevel meir enn begge desse områda.

- It-tryggleik reknast ofte som den tekniske delen av informasjonstryggleik. Det er sikring av informasjonssystema som gjerast på nettverks- eller systemnivå. Informasjonstryggleik omfattar i tillegg tiltak som t.d. fysisk tryggleik (dørlåsar, tilgangskontroll), personellstyring (opplæring, referansekontroll), juridisk støtte, organisasjon, prosessar, osb.

- Vern av personopplysningar er ein viktig del av informasjonstryggleiksarbeidet. Det er likevel mykje annan informasjon som òg må og bør vernast i ein organisasjon. For HFK er dette til dømes anbod- og tilbodsinformasjon eller politiske saker som ikkje er klare for handsaming.

Krav i gjeldande lover
Personopplysningsloven og –forskriften stiller ein del krav til handsaming av personopplysningar. Desse krava bør gå inn i eit styringssystem (internkontrollsystem) for informasjonstryggleik, som òg bør gjerast gjeldande for anna informasjon som skal vernast.

Personopplysningsforskriften § 2-3 *Sikkerhetsledelse*
- *Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges.*
- *Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål.*
- *Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.*
- *Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.*
- *Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.*