Informasjonssikkerhet i Nord-Trøndelag fylkeskommune

Nord-Trøndelag fylkeskommune tar i bruk stadig flere it-løsninger for å ivareta en effektiv tjenesteproduksjon. Samtidig som at slike løsninger letter tilgang informasjon, gjør disse oss også sårbar dersom ulike typer informasjon forvaltes på en feilaktig måte eller kommer på avveie.

Nord-Trøndelag fylkeskommune legger stor vekt på å ivareta informasjonssikkerheten på en helhetlig og forsvarlig måte. Dette gjelder tilstrekkelig sikkerhet knyttet til behandling av personinformasjon og virksomhetssensitiv informasjon iht krav definert i Lov om personopplysninger med tilhørende forskrifter.

Dette krever at hele organisasjonen har fokus og kompetanse på lovverk og retningslinjer, og har gode rutiner der person- og virksomhetssensitiv informasjon behandles.

Hva er informasjonssikkerhet?

Informasjonssikkerhet omfatter tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet), og at informasjon er til stede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).

Informasjonssikkerhet omfatter tiltak rettet mot sikring av

- personopplysninger, iht Lov om personopplysninger med forskrifter
- virksomhetssensitiv informasjon, iht Lov om Lov om offentlig forvaltning
- NTFK's driftssituasjon, tjenesteproduksjon og verdier

Behandling av personopplysninger i NTFK

Med personopplysninger menes alle opplysninger og vurderinger som direkte eller indirekte kan knyttes til en enkeltperson.

Alle personopplysninger skal behandles i forhold til krav som stilles i Personopplysningsloven med tilhørende forskrifter. For Nord-Trøndelag fylkeskommunes vedkommende vil slik behandling i hovedsak omfatte:

- Elevopplysninger – vedr elever i videregående opplæring og voksenopplæring
- Personalopplysninger – vedr ansatte i NTFK
- Pasientopplysninger – vedr tannhelsebehandling
- Innbyggeropplysninger – vedr søknadsbehandling etc

En del av de opplysninger karakteriseres som sensitive personopplysninger, som er underlagt spesielt strenge sikkerhetstiltak. Sensitive personopplysninger er opplysninger om:

- Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
- Helseforhold,
- Seksuelle forhold,
- Medlemskap i fagforeninger

I tillegg skal ikke fødselsnummer (11 sifre) benyttes i andre tilfeller enn der det er høyst nødvendig for å identifisere en person.

Nord-Trøndelag fylkeskommunes målsetning med informasjonssikkerhet

NTFK's hovedmålsetning for behandling av personopplysninger er å ivareta kravene i Lov om personopplysninger, herunder å hindre at den enkeltes personvern kompromitteres ved å sikre at:

1. kun autoriserte medarbeidere med legitime behov har tilgang til informasjon og ressurser (Konfidensialitet)

2. autoriserte medarbeidere har tilgang til korrekte ressurser og informasjon til rett tid og i riktig omfang (Tilgjengelighet)

3. kvaliteten på informasjonen er gyldig, nøyaktig og fullstendig (Integritet)

Risikoprofil for behandling av personopplysninger

1. For å hindre at personopplysninger kompromitteres skal sikkerhetstiltak etableres slik at det blir lav sannsynlighet for at hendelser som kan medføre store konsekvenser for enkeltmenneskers personvern inntreffer.
2. For personopplysninger som medfører liten konsekvens for enkeltmenneskers personvern aksepterer NTFK høyere grad av sannsynlighet for at uønskede hendelser inntreffer.

Overordnede rutiner knyttet til behandling av personopplysninger

NTFK skal behandle personopplysninger i samsvar med kravene i personopplysningsloven.

Ingen personopplysninger skal samles inn/ behandles/ lagres mv uten:

1. at det er fastsatt ved lov at det er adgang til slik behandling,
2. eller at opplysningene innhentes for å ivareta en berettiget interesse,
3. eller at den opplysningene omhandler har gitt sitt samtykke

En hver som henvender seg til en av NTFK's virksomheter og ber om det skal få opplysninger om hvilke typer personopplysninger som behandles/ er registrert om dem selv.

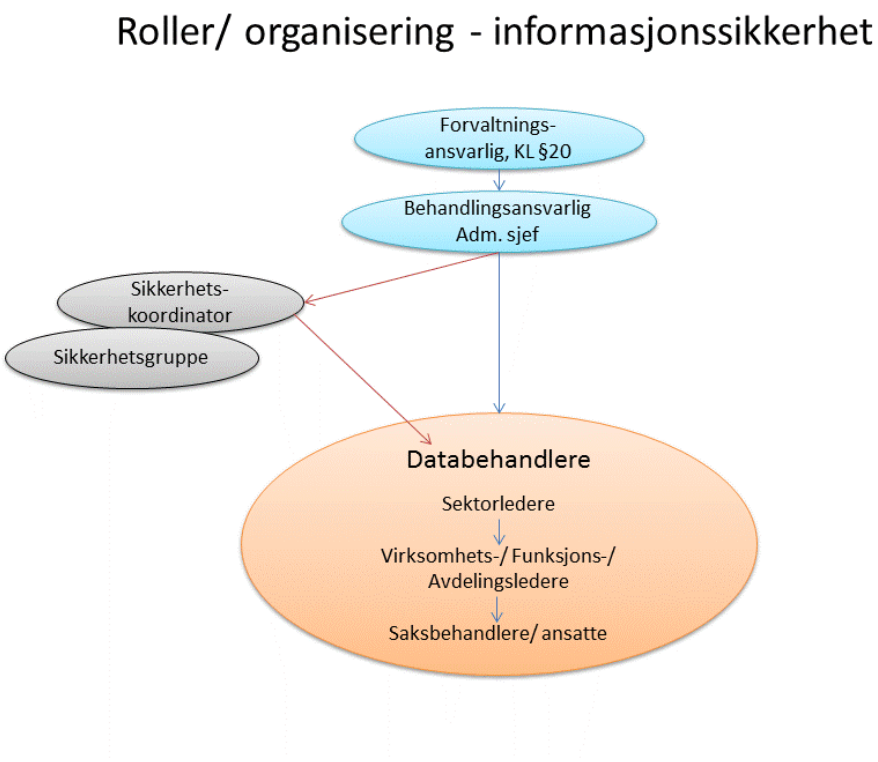
Viktige prinsipper for informasjonssikkerhetsarbeidet

I NTFK's virksomheter skal følgende prinsipper legges til grunn for sikkerhetsarbeidet:

1. Risikoen for at uønskede hendelser skal inntreffe identifiseres gjennom risikovurdering.
2. Nye og endrede trusler skal identifiseres og vurderes fortløpende.
3. Sikkerhetstiltakene skal til enhver tid stå i forhold til akseptabelt risikonivå.
4. Når uønskede hendelser inntreffer skal beredskapstiltak bidra til å begrense skaden og til rask reetablering av normal drift.
5. Sikkerhetsarbeidet skal integreres i arbeidet i linjen.
6. God sikkerhet skal bygge på riktige holdninger blant medarbeiderne.
7. Alle ansatte skal få nødvendig opplæring for å ivareta sitt sikkerhetsansvar.
8. All tilgang til informasjon og verdier skal være basert på tjenestelige behov.

Ansvar og roller

Ansvaret for informasjonssikkerheten ivaretas etter følgende organisering:



1. Nord-Trøndelag fylkeskommunes databehandlingsansvarlige iht Lov om Personopplysninger §2, punkt 4 er administrasjonssjefen etter fullmakt fra Fylkesrådet.

2. Informasjonssikkerhetsarbeidet ivaretas gjennom et samlet Internkontrollsystem i NTFK.
3. Det er oppnevnt en sikkerhetskoordinator og etablert en sikkerhetsgruppe, som har i oppgave å iverksette og koordinere tiltak for å ivareta en samlet informasjonssikkerhet på en forsvarlig måte. Det bør også finnes en person som ivaretar slik koordinering på den enkelte virksomhet.
4. Ledelsens/ behandlingsansvarliges gjennomgang knyttet til informasjonssikkerhet gjennomføres en gang pr år i forbindelse med annen årsrapportering.
5. Informasjonssikkerhetsarbeidet ivaretas delegert i linjeorganisasjonen, og ledelsen ved den enkelte virksomhet skal sørge for at dette ivaretas på en forsvarlig måte i henhold til sentrale føringer.
6. I følge personopplysningsloven § 2 punkt 5 er databehandleren *«den som behandler personopplysninger på vegne av den behandlingsansvarlige»*.
   a. Alle ledere i NTFK må påse at ansatte som behandler personopplysninger og virksomhetssensitiv informasjon er kjent med sitt ansvar som databehandler og innehar tilstrekkelig kompetanse for å ivareta dette.
   b. Alle systemeiere må påse at leverandører som gjennom sine oppdrag kommer i kontakt med personopplysninger eller virksomhetssensitiv informasjon har undertegnet databehandleravtale, og at slike leverandører har rutiner som ivaretar informasjonssikkerheten på en forsvarlig måte.

Avviksbehandling

Som avvik regnes en hver hendelse eller tilstand som bryter med NTFK's internkontroll mht ivaretakelse av informasjonssikkerhet. Dette omhandler både bevisst og ubevisst rutinesvikt, regelbrudd eller angrep som truer fylkeskommunens tjenesteproduksjon eller verdier.

- Alle ansatte i NTFK har plikt til å varsle avvik som de oppdager gjennom rapportering til nærmeste leder.
- Ledere er ansvarlig for umiddelbart å iverksette strakstiltak for å stoppe avviket og begrense skadeomfanget, evt i samarbeid med berørte parter eller IT-funksjon.
- Avvik rapporteres umiddelbart på eget elektronisk skjema som sendes via virksomhetsledelsen og videre til virksomhetens sikkerhetskoordinator.
- Alle avvik rapporteres periodisk til sikkerhetskoodinator. Ved alvorlige avvik eller ved uautorisert utlevering av personopplysninger skal sikkerhetskoordinator varsles umiddelbart. Denne vil varsle Datatilsynet dersom dette er påkrevet.

Behandling av sensitive personopplysninger i NTFK

Sensitive personopplysninger skal behandles i sikret sone for å sikre at slik informasjon ikke kommer på avveie. Alle sentrale og lokale sikringstiltak skal være dokumentert. Det er viktig at det fokuseres på å opprettholde en forsvarlig sikkerhet knyttet til dette, som omfatter:

- Personellsikring
    - Krav til kompetanse
    - Taushetsplikt
    - Autorisasjon
- Fysisk sikring
    - Arealer hvor kun spesielt godkjente (autoriserte) medarbeidere har adgang (serverrom, arbeidsplass, printere, scannere etc)
- Systemteknisk sikkerhet
    - Sone der sensitive personopplysninger behandles. Den enkelte sikrede sone skal være sikkerhetsmessig adskilt fra resten av det interne nettverket og fra evt andre sikrede soner med tekniske sikkerhetsbarrierer.

Nord-Trøndelag fylkeskommune har behandlet personopplysninger i to sikrede soner i flere år; en for elevopplysninger knyttet til bruk av systemene OTTO og HK-data, og en for pasientopplysninger tilknyttet tannhelse med pasientjournalsystemet Opus.

Innføring av ny versjon av sak-/ arkivsystemet 360°

I forbindelse med innføring av ny versjon av 360° vil dokumenter med sensitivt innhold bli tatt inn i sak-/ arkivsystemet. Det betyr at dette systemet blir tilknyttet to sikrede soner:

- Sikret sone for elevopplysninger
- Sikret sone for personalopplysninger

Systemet i sikret sone vil bli installert i løpet av juni 2012, og vil bli gjort tilgjengelig for brukere etter hvert som andre forutsetninger har kommet på plass.

- Skolene må sørge for forsvarlig sikring og skjerming av brukerstedene.
- Leder oversender søknad om tilgang til aktuell sikret sone for brukere de mener har et tjenestelig behov for dette. For å imøtekomme gjeldende bestemmelser må følgende krav stilles til brukere i sikret sone:
    - Konkrete tjenestelige behov (ikke på grunnlag av tittel/ rolle)
    - Behov over et visst minimumsomfang (daglig/ ukentlig)
    - Kunnskap om informasjonssikkerhet
    - Vurdering ift minimumskrav til systemkompetanse/ -forståelse

- Underskrevet taushetserklæring
- Gjennomgått sikkerhetsinstruks

For at ikke brukerne skal måtte benytte egne pcer i sikret sone vil tilgang til systemene bli gitt gjennom egen pålogging via terminalserverløsning, og det vil ikke være mulig å være pålogget flere soner samtidig. Dette betyr at brukerne vil kunne ha flere brukerkontoer de skal ha tilgang til; en til intern sone og en til hver av sikrede soner. Sikret sone vil ikke bli gjort tilgjengelig i trådløse nett.

Scanning i sikret sone vil i første omgang kun foregå som en pilot i sentralarkivet.

Det må settes opp egne skrivere i sikret sone med samme krav til skjerming fysisk sikring som ellers i sikret sone. Det frarådes å benytte multifunksjonsskrivere i sikret sone.

Konklusjon.

Administrasjonssjefen ber om at sikkerhetsarbeidet tas inn i arbeidet og organiseringen i virksomheten. Det vil bli utarbeidet mer detaljerte retningslinjer i tiden som kommer for hvordan NTFK skal ivareta informasjonssikkerheten på en forsvarlig måte. Alle retningslinjer vedrørende dette må følges opp lokalt og implementeres i arbeidet i virksomheten.