Overordnede retningslinjer for Informasjonssikkerhet

i

Nord-Trøndelag fylkeskommune

Versjon	1.0
Dato	10.12.2014
Utarbeidet av	Sikkerhetskoordinator

Innhold

1. Ledelsens formål med informasjonssikkerhet

Informasjonsteknologi og sikkerhet er vesentlig for at Nord-Trøndelag fylkeskommune (NTFK) skal kunne yte tjenester for innbyggere, tjenestemottakere og ansatte, og er et kritisk virkemiddel for effektive arbeidsprosesser. Det stilles derfor strenge krav til at sikkerheten blir tilstrekkelig ivaretatt. Systemer og infrastruktur skal være pålitelige i bruk, samtidig som at informasjon skal være tilgjengelig, korrekt og beskyttet mot uautorisert tilgang.

NTFKs medarbeidere, skoleelever og andre brukere skal alltid kunne motta korrekt informasjon til riktig tid. Samtidig som at alle skal være trygge på at informasjonen som trenger beskyttelse blir behandlet på korrekt måte i samsvar med personopplysningsloven og andre bestemmelser, og etter metoder fra internasjonale standarder for informasjonssikkerhet.

Dette betyr at NTFK skal ha tiltak som sikrer at informasjon og informasjonssystemer er beskyttet mot uønskede hendelser – som eksempel på dette nevnes menneskelige feil, feil på utstyr, hacker- eller virus-angrep, innbrudd, strømsvikt, brann etc.

Dette dokumentet oppfyller føringer for kvalitetsarbeidet i NTFK i forhold til informasjonssikkerhet. Overtredelse av disse retningslinjer for informasjonssikkerhet og vedtatte sikkerhetskrav ansees å være et tillitsbrudd mellom ansatte og NTFK. Ved alvorlige overtredelser vil ansettelsesforholdet bli vurdert.

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.

Inge Fornes

Administrasjonssjef i Nord-Trøndelag fylkeskommune

2. RAMMER OG MÅL FOR INFORMASJONSSIKKERHET

2.1. Omfang og definisjoner

Disse retningslinjene omhandler informasjonssikkerhet, fysisk sikkerhet og personellsikkerhet for hele NTFK, og gjelder for alle personer som behandler eller har tilgang til data og/eller informasjon som eies eller forvaltes av NTFK.

Retningslinjene omfatter også alle tilganger til systemer som finnes i NTFKs nettverk, og kravene til sikkerhet gjelder for all informasjon enten den er elektronisk eller papirbasert

Informasjonssikkerhet omfatter beskyttelse mot avvik mht.:

- **konfidensialitet**; sikkerhet for at kun autoriserte personer har tilgang til sensitiv informasjon, og at den ikke avsløres til uvedkommende
- **integritet**; sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter
- **tilgjengelighet**; sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov
- **sporbarhet**; for alle systemer som er installert i sikret sone skal ha funksjonalitet som gjør det mulig i ettertid å konstatere hva som er gjort i et dataanlegg/ informasjonssystem, herunder hvem som har fått tilgang til opplysningene.

Informasjonssikkerhet omfatter tiltak rettet mot sikring av personopplysninger, iht Lov om personopplysninger med forskrifter, virksomhetssensitiv informasjon, iht Lov om Lov om offentlig forvaltning, offentlighetslov og arkivlov, samt NTFKs driftssituasjon, tjenesteproduksjon og verdier.

2.2. Overordnede krav

2.2.1. Eksterne krav

NTFK skal følge gjeldende lovverk, samt andre eksterne retningslinjer, slik som (ikke avgrenset til):

- Lov om behandling av personopplysninger (Personopplysningsloven) med forskrifter
- Lov om kommuner og fylkeskommuner (Kommuneloven)
- Lov om behandlingsmåten i forvaltningssaker (Forvaltningsloven)
- Lov om rett til innsyn i dokument i offentleg verksemd (Offentleglova)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Lov om elektronisk signatur (eSignaturloven)
- Lov om arkiv (Arkivlova) m/forskrifter
- Datatilsynets krav

2.2.2. Interne sikkerhetsbestemmelser

- Alle ansatte og elever skal forholde seg i overensstemmelse med *Retningslinjer for informasjonssikkerhet* med tilhørende IKT-reglement.
- Oppfølging av dette er linjeledelsens ansvar.
- Ansatte og elever skal være informert om at bevis fra sikkerhetshendelser kan bli tatt vare på (lagret) og overleveres til politi eller påtalemyndigheter etter rettslig krav.

- Gjennomføring av revisjoner skal planlegges og avtales med de involverte for å minimalisere risikoen for at NTFKs aktiviteter blir forstyrret.

2.3. Målsettinger

Korrekt informasjon i NTFK er tilgjengelig for autorisert intern eller ekstern person eller system, når som helst, fra hvor som helst, og med mange informasjonskilder/-verktøy.

Dette innebærer mer konkret at arbeidet med informasjonssikkerhet skal:

1. Støtte og effektivisere saks- og brukerbehandlingen.
2. Oppfylle gjeldende lov- og regelverk.
3. Sørge for at informasjon er tilgjengelig når den trengs.
4. Unngå at personopplysninger om tjenestebrukere, deres familie og nettverk eller taushetsbelagt informasjon kommer på avveie.
5. Beskytte ansatte mot hendelige uhell i informasjonsbehandlingen og unngå hendelser som reduserer NTFKs omdømme.

2.3.1. Mål for sikkerhetsarbeid i NTFK

Tilgjengelig og korrekt informasjon, informasjonssystemer og sikkerhet generelt er kritisk og svært viktig for NTFK. Hovedmålet med sikkerhetsarbeidet er å ivareta NTFKs, ansattes, skolelever og andre brukeres krav til konfidensialitet, integritet, tilgjengelighet og sporbarhet.

NTFKs hovedmålsetning for behandling av personopplysninger er å ivareta behovet for tilgjengelig og korrekt informasjon, samt krav til informasjonssikkerhet i lovverket.

NTFK skal ha gode rutiner som bidrar til å forebygge sikkerhetsbrudd.

2.3.2. Delmål for informasjonssikkerhet i NTFK

- Å etablere kontroller for å beskytte NTFKs informasjon og informasjonssystemer mot tyveri, misbruk og andre former for skade eller tap.
- Å etablere ansvar og eierskap for informasjonssikkerhet i NTFK.
- Å motivere ledelse, ansatte og elever til å opprettholde kunnskap og kompetanse om sikkerhet, slik at frekvens og skadenivå av sikkerhetshendelser kan minimaliseres.
- Å sikre at NTFK er i stand til å fortsette sine tjenester, også i fall større hendelser i forhold til informasjonssikkerhet skulle inntreffe.
- Å bidra til at personvernet ivaretas, og at NTFK kan gjennomgå tilsyn uten avvik.

Brudd på lovverk og interne retningslinjer kan skade NTFKs informasjon og infrastruktur.

Videre kan brudd føre til at informasjon som er eid eller forvaltet av NTFK blir misbrukt eller ødelagt. Dette kan påføre NTFK straffe- eller erstatningsansvar, inndragning av konsesjon for personregistre, krav om forvaltningsbøter, eller på annen måte skade NTFKs interesser og omdømme.

Overtredelser av retningslinjer/ sikkerhetskrav vil derfor være et tillitsbrudd mellom brukeren og NTFK, og vil kunne medføre konsekvenser for ansettelses- eller studieforholdet.

2.4. Særlige krav til behandlingen av personopplysninger

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 (POL) 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 er i loven definert som sensitive personopplysninger, og er underlagt spesielt strenge sikkerhetstiltak. Jfr POL §2.8 og §9.

I tillegg skal bruk av fødselsnummer (11 sifre) kun benyttes i tilfeller enn der det er høyst nødvendig for å identifisere en person. Jfr POL §11.

2.5. Tiltaksområder

Strategier og tiltak på følgende 10 områder skal sørge for at NTFK oppnår vedtatte mål for informasjonssikkerhet:

1. **Tjenestebrukere**
   Brukere av NTFKs tjenester skal være kjent med sine rettigheter. De skal kunne stole på at informasjonsbehandling og -formidling utføres i tråd med tjenestebrukernes behov og retningslinjer for informasjonssikkerhet.

2. **Ansatte**
   Alle ansatte i NTFK skal være autorisert for og ha kompetanse i bruk av informasjonssystemene, og er i henhold til Forvaltningslovens §13 pålagt taushetsplikt. Medarbeidere skal følge lovverk, eksterne og interne retningslinjer om informasjonssikkerhet og utføre sin informasjons-behandling i tråd med dette. Sanksjoner ved brudd skal være kjent.

3. **Samarbeidspartnere**
   Alle eksterne forbindelser som inngår i NTFKs informasjonsbehandling skal, der dette er naturlig, være kjent med og følge krav til informasjonssikkerhet i NTFK. Det skal inngås databehandleravtale med eksterne samarbeidspartnere som kommer i befatning med personopplysninger eller annen taushetsbelagt informasjon som NTFK har forvaltningsansvar for å forsikre seg om at partneren har tilstrekkelig informasjonssikkerhet.

   Offentligheten skal være kjent med at informasjonsbehandling i NTFK utføres i tråd med etablert praksis og retningslinjer for informasjonssikkerhet, herunder nødvendige registreringer hos Datatilsynet.

4. **Personopplysninger og annen taushetsbelagt informasjon**
   Det skal føres oversikt over hvilke personopplysninger som behandles i NTFK. Det skal etableres krav til tilgjengelighet, konfidensialitet, integritet, og sporbarhet i informasjonsbehandlingen og i informasjonsinfrastrukturen. Det skal gjennomføres tiltak som muliggjør at kravene innfris. Krav

og tiltak for å innfri disse, skal være basert på risikovurderinger og stå i forhold til sannsynligheten for og konsekvens av brudd på informasjonssikkerhet i saks- og brukerbehandlingen. Tiltakene skal omfatte nødvendig fysisk sikring samt kontinuitet og beredskap. Nye risikovurderinger skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

5. **Organisering**
   Organisering og ansvar for informasjonssikkerhet i saks- og brukerbehandlingen i NTFK skal være beskrevet, operasjonalisert og kjent for alle relevante brukere.

6. **Regelverk**
   I tillegg til det overordnede regelverket, skal det utarbeides og foreligge lokale informasjonssikkerhetsregelverk i den enkelte enhet i NTFK. For å innfri strategiene skal det implementeres regelverk (retningslinjer og regler, standarder, veiledninger, rutiner og prosedyrer) for informasjonssikkerhet i NTFK.

7. **Hendelser og avvik**
   System og rutiner for håndtering av hendelser og avvik skal være etablert og kjent.

8. **Revisjon**
   Sikkerhetsrevisjon av bruk av informasjonssystemene i NTFK skal gjennomføres jevnlig, eksempelvis årlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, informasjonssikkerhetstiltak, regelverk, bruk av informasjonssystemene samt bruk av kommunikasjonspartner og leverandører. Den enkelte virksomhet i NTFK skal jevnlig gjennomgå sin informasjonssikkerhetsstatus (internkontroll) og årlig rapportere status til sikkerhetskoordinator.

9. **Ledelsens styring og oppfølging**
   Hovedaktiviteten «Ledelsens styring og oppfølging» utføres gjennom følgende aktiviteter:
   - Bestille og vurdere analyse av status
   - Bestille og iverksette plan for bedre internkontroll og informasjonssikkerhet
   - Utforme overordnede, styrende dokumenter
   - Ledelsens gjennomgang (minimum en gang pr. år)
   - Utforme styringsparametre og årlige krav
   - Godkjenne og finansiere risikohåndteringsplaner og tiltak
   - Krise- og beredskapshåndtering
   -

3. PRINSIPPER FOR ARBEIDET MED INFORMASJONSSIKKERHET

Viktige prinsipper for informasjonssikkerhetsarbeidet er at:

- Sikkerhetsarbeidet skal integreres i arbeidet i linjen.
- God sikkerhet skal bygges på riktige holdninger blant medarbeiderne.
- Alle ansatte skal få nødvendig opplæring for å ivareta sitt sikkerhetsansvar.
- All tilgang til informasjon og verdier skal være basert på tjenestelige behov.

3.1. Risikostyring

NTFK definerer risiko som kombinasjonen av sannsynligheten for at en hendelse skal inntreffe og konsekvensen av den.

- Risikoen identifiseres gjennom risikovurdering.
- Nye trusler skal identifiseres og vurderes fortløpende.
- Ved innføring av nye systemer skal behovet for risikoanalyse vurderes. Dersom systemet behandler personopplysninger skal risikovurdering alltid gjennomføres.
- Sikkerhetstiltakene skal til enhver tid stå i forhold til akseptabelt risikonivå.

3.2. Avviksbehandling

Som avvik regnes enhver hendelse eller tilstand som bryter med NTFKs 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. Avvik rapporteres videre til sikkerhetskoordinator.
- Når uønskede hendelser inntreffer, skal beredskapstiltak bidra til å begrense skaden og raskt komme tilbake til normal drift.

3.3. Klassifisering og kontroll

Krav til åpenhet og tilgang til informasjon er regulert i Offentlighetsloven. Informasjon og infrastruktur skal klassifiseres med hensyn til sikkerhetsnivå og tilgangsbegrensning.

Informasjonen skal klassifiseres i en av tre følgende kategorier for konfidensialitet:

- **Sensitiv**
  Informasjon av sensitiv art hvor uautorisert tilgang (også internt) kan medføre betydelig skade for enkeltpersoner, fylkeskommunen eller deres interesser.

- **Unntatt offentlighet**
  Informasjon som kan skade NTFK eller være upassende at tredjepart får kjennskap, herunder som kommer under forvaltningslovens «Unntatt Offentlighet» eller informasjon som NTFK selv definerer som begrenset.

- **Åpen**
  All annen informasjon er åpen.

3.4. Fysisk og miljømessig sikkerhet

Sikkerhetsområder

For å sikre konfidensialitet skal sikre fysiske soner benyttes for å beskytte områder som inneholder IKT-utstyr og informasjon som krever beskyttelse. Sikre soner skal beskyttes med hensiktsmessige adgangskontroller for å sikre at kun autorisert personell får adgang.

Maskinrom, kommunikasjonsrom og lignende områder skal være avlåst med adgangskontroll og logging, og være kun tilgjengelig for autorisert personell. Eksternt servicepersonell som har behov for tilgang skal følges av autorisert person.

Maskinrom skal være utstyrt i henhold til vedtatte standarder i NTFK.

3.5. Driftsadministrasjon i NTFK

Prosedyrer og ansvarsområder

- Implementering av IKT-utstyr og programvare skal gjennomføres i henhold til vedtatte standarder og sikkerhetskrav i NTFK.
- IT-avdelingen og systemeiere skal sikre dokumentasjon av IKT-systemer.
- Endringer i IKT-systemer skal kun gjennomføres dersom det er virksomhetsmessig og sikkerhetsmessig velbegrunnet.
- Driftsoppgaver skal være skriftlig dokumentert i egne prosedyrer. Denne dokumentasjonen skal oppdateres etter alle vesentlige endringer.
- Oppgaver og ansvar skal separeres på en slik måte at det reduserer muligheten for uautorisert eller uforutsett misbruk av NTFKs eiendeler/systemer.
- IT-avdelingen skal sørge for at det foreligger en beredskapsplan for å minimalisere konsekvens og sannsynlighet for feilsituasjoner i IT-systemene.
- IT-avdelingen er ansvarlig for regelmessig sikkerhetskopiering og testing av denne, samt oppbevaring av data på NTFKs IKT-systemer iht. klassifisering.
- Sikkerhetskopier skal oppbevares eksternt eller i egen relevant sikret sone.

3.6. Systemutvikling og vedlikehold

Definisjoner av virksomhetsmessige krav til nye systemer eller videreutvikling av systemer skal inneholde sikkerhetsmessige krav.

De systemer som utvikles for eller av NTFK skal ha klare krav til sikkerhet, inkludert validering av data og sikring av koden før produksjonssetting.

All programvare skal gjennomtestes og aksepteres formelt av systemeier og IT-avdelingen før programvaren overføres til produksjonsmiljøet.

3.7 Risikovurdering

Før større endringer i sentrale systemer skal det gjennomføres en risikovurdering. Dersom risiko vurderes som uakseptabel skal det iverksettes tiltak eller vurdere alternative løsninger som medfører lavere risiko.

3.8 Personellsikkerhet

Ved ansettelse

- Sikkerhetsansvar og -roller for relevant personell, både ansatte og innleide, skal beskrives av nærmeste overordnede.
- Arbeidsavtale som signeres av alle ansatte i NTFK henviser til Forvaltningslovens §13 angående taushetsplikt.
- IKT-reglementet skal aksepteres i alle ansettelsesforhold og ved systemtilganger for tredjepart.

For brukere gjelder

- IKT-reglementet refererer til NTFKs krav til informasjonssikkerhet og brukernes ansvar for å oppfylle disse.
- IKT-reglementet skal gjennomgås jevnlig med alle brukere og ved alle nyansettelser.
- Den ansattes har plikt å påse at en har nødvendig kompetanse til å håndtere de informasjonssystemer som jobben krever.
- Brudd på retningslinjer for informasjonssikkerhet vil normalt medføre sanksjoner i henhold til NTFKs reglement og retningslinjer. For ansatte henvises også til tjenestemannsloven.
- NTFKs informasjon, informasjonssystemer og utstyr skal kun benyttes til de formål de er bestemt for.
- Bruk av NTFKs IKT-infrastruktur i egen næringsvirksomhet er ikke tillatt med mindre det er særskilt godkjent av Administrasjonssjefen.
- Alle ledere i NTFK må påse at ansatte som behandler personopplysninger og virksomhets-sensitiv informasjon er kjent med sitt ansvar som databehandler og innehar tilstrekkelig kompetanse for å ivareta dette.

Avslutning eller endring av ansettelse

- Ansvar for avslutning eller endring av ansettelsesforhold skal være klart definert i en egen rutine.
- NTFKs eiendeler skal leveres inn ved opphør av tjenestelig behov for bruk av eiendelene dersom det ikke er gjort avtale om utkjøp.
- NTFK skal endre eller stenge tilgangsrettigheter ved opphør av ansettelse eller endring av arbeidsforhold.
-

3.9. Tilgangskontroll

Alle ansatte utstyres med personlig datautstyr som er tilpasset rolle og funksjon. Dette skal kun brukes av arbeidstaker selv, og skal sikres mot at uautoriserte får tilgang.

Det tillates ikke at utstyr som ikke er klarert for bruk i NTFKs nett får tilgang til interne ressurser.

Det skal finnes en skriftlig tilgangs- og passordpolicy som er basert på virksomhets- og sikkerhetsmessige krav og behov. Denne skal revideres regelmessig.

IT-sjef har myndighet til å fastsette krav til nødvendige sikkerhetstiltak knyttet til mobile enheter som kan gis tilgang til NTFKs nettverk.

3.10. Kontinuitetsplanlegging (beredskap)

Dersom en kritisk situasjon oppstår, for eksempel ved at kritiske IT-systemer ikke fungerer, eller ved at andre hendelser gir alvorlige forstyrrelser på virksomhetens normale operasjon skal alternative rutiner tas i bruk.

Det skal finnes en plan som beskriver de alternative rutinene som virksomheten må følge når en kritisk situasjon har oppstått. Slike rutiner skal finnes for de mest kritiske tjenestene i NTFK som derfor må identifiseres og prioriteres.

Kontinuitetsplanen skal dokumentere de normale forretningsprosessene på en overordnet måte og inneholde rutinebeskrivelser som skal dekke følgende formål:

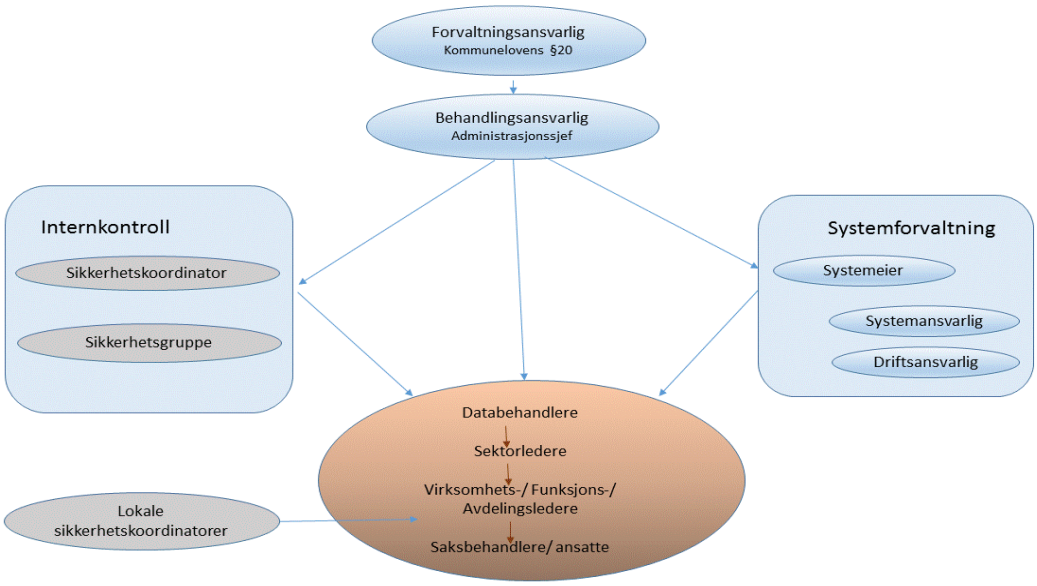
- minimalisere tapt tjenesteproduksjon eller økonomiske tap som en direkte følge av hendelsen
- opprettholde de viktigste tjenestene ved å ta i bruk alternative rutiner
- retur til normal virksomhet

4. ROLLER OG ANSVAR FOR INFORMASJONSSIKKERHET

4.1. Organisering av informasjonssikkerheten

Informasjonssikkerhetsarbeidet i NTFK er organisert gjennom en informasjonssikkerhetsstrategi med fordeling av roller og ansvarsområder som er definert slik:

- Fylkeskommunes databehandlingsansvarlige iht Lov om Personopplysninger §2.4 er Fylkesrådsleder, men er delegert til Administrasjonssjef.
- Informasjonssikkerhetsarbeidet ivaretas gjennom Internkontrollen i NTFK.
- Det er oppnevnt sikkerhetskoordinator og sikkerhetsgruppe som har som oppgave å iverksette tiltak for å ivareta informasjonssikkerheten.
- IT-sjef har ansvaret for sikkerheten ved den tekniske driften.
- Informasjonssikkerhetsarbeidet ivaretas i linjeorganisasjonen, og det er den enkelte virksomhetsleders ansvar å sørge for at dette ivaretas på en forsvarlig måte. Ansvar for lokalt sikkerhetsarbeid skal plasseres og utøves.
- Den enkelte ansatte er ansvarlig gjennom linjeorganisasjonen og som er definert gjennom retningslinjer, taushetserklæring og en rekke sikkerhetsprosedyrer. Ansatte skal gjøre seg kjent med dette dokumentet og lovpålagte og interne retningslinjer for informasjons-sikkerhet.
- Ledelsens gjennomgang gjennomføres en gang pr år i tilknytning til annen årsrapportering.



I følge personopplysningsloven § 2 punkt 5 er databehandleren *«den som behandler person-opplysninger på vegne av den behandlingsansvarlige»*.

- Alle ledere i NTFK skal påse at ansatte som behandler personopplysninger og virksomhetssensitiv informasjon er kjent med sitt ansvar som databehandler og innehar tilstrekkelig kompetanse for å ivareta dette.
- Systemeiere har et overordnet juridisk ansvar for bruken av systemet, og at dette brukes i samsvar med gitte retningslinjer. Disse må også påse at leverandører som gjennom sine oppdrag kommer i kontakt med personopplysninger eller virksomhetssensitiv informasjon har undertegnet databehandleravtale, og at leverandører som skal ha tilgang til NTFKs databaser har rutiner som ivaretar informasjonssikkerheten på en forsvarlig måte.

4.2. Sikkerhetsgruppe

Som en del av internkontrollen er det opprettet en sikkerhetsgruppe med en sikkerhetskoordinator som har som oppgave å koordinere arbeidet med informasjonssikkerhet i NTFK. I tillegg skal en lokal sikkerhetskoordinator ivareta det daglige sikkerhetsarbeidet på virksomheten, gjerne støttet av en gruppe med representanter fra ulike brukergrupper.

Rapport fra ROS-analysen 2013 vil være et grunnlag for arbeidet som sikkerhetsgruppa skal starte opp. Her skal det prioriteres tiltak som gjør at NTFK oppfyller de minimumskrav som er stilt i Lov om personopplysninger med forskrifter, samt Datatilsynets veiledere på området. Videre skal gruppa identifisere, vurdere og sørge for gjennomføring av tiltak mot de alvorligste trusler innenfor fylkeskommunens tjenesteproduksjon og omdømme.

Sikkerhetsorganisasjonen skal ivareta både hensynet til lovverkets bestemmelser og til de løpende sikkerhetsutfordringer som fylkeskommunens tjenesteproduksjon utsettes for.