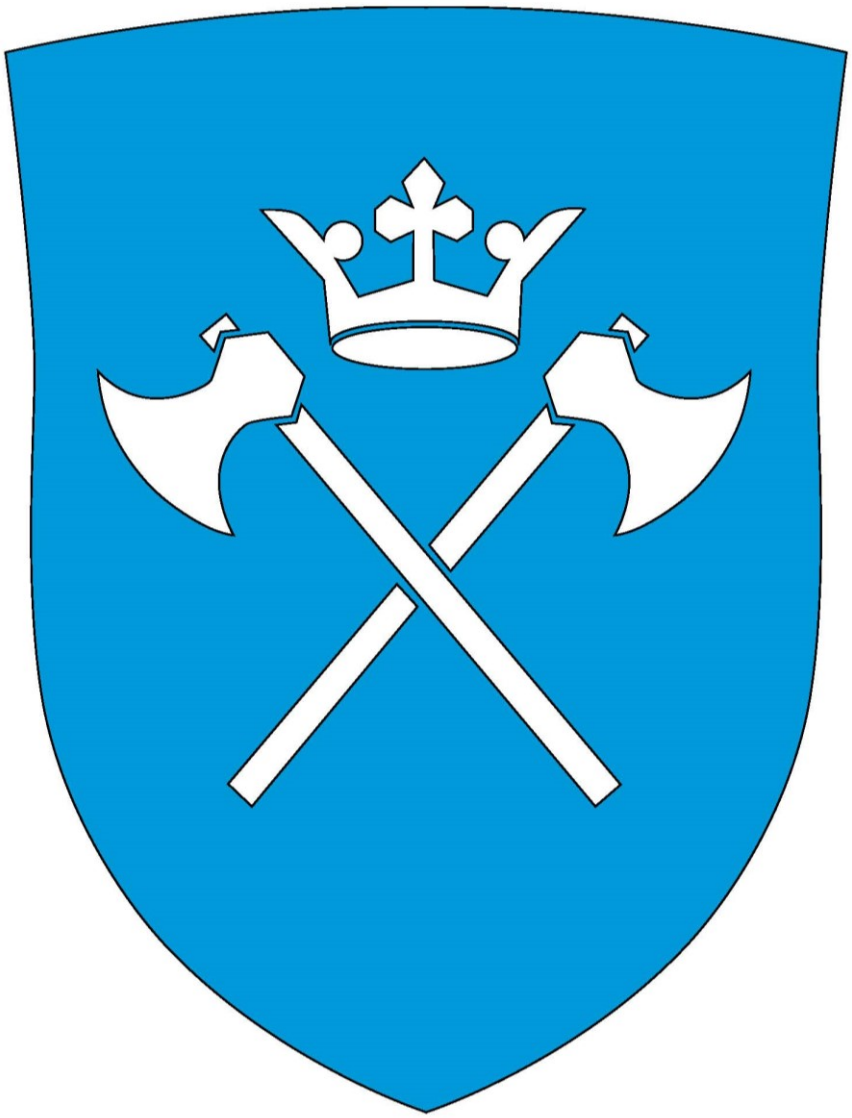

Handbok i Informasjonstryggleik for Tysnes kommune

2022

Innhaldsliste

1 Innleiing

Informasjonstryggleikt handlar om sikring av informasjonsverdiar som gjeld både offentleg forvaltning, verksemder, organisasjonar og enkeltpersonar. Difor gjeld det oss alle.

Tilgang til informasjon og informasjonssikring skal ikkje vera to motstridande interesser. Målet med informasjonssikring er å sikra informasjonen mot misbruk.

1.1 Krav til sikring av informasjon

Krava til sikring av informasjon blir bestemt i hovudsak av to faktorar:

A. innhaldet i informasjonen
B. kva samanheng han blir behandla i

Den største trusselen mot Informasjonstryggleik er primært oss menneske og den manglande forståinga vår for behovet for sikring. Det kan handla om manglande sikring eller om manglande kompetanse. Sikringstiltak, systematikk, rutinar og prosedyrar skal vareta informasjonstryggleik på ein formell, systematisk og etterprøvbar måte.

Informasjonstryggleik er knytt til behandling av personopplysningar. Innhaldet her gjeld behandling av både sensitive og ikkje sensitive personopplysningar om tilsette, elevar, barnehagebarn, tenestemottakarar og andre som kommunen behandlar personopplysningar om.

Det er viktig å ha ein lovleg grunn til å behandla personopplysningar. Grunnlag for behandling er normalt basert på lovheimel eller samtykke frå den registrerte. Uavhengig av grunnlaget, har verksemda plikt til å informera den registrerte om korleis ho har tenkt å behandla opplysningane. Det betyr at det må informerast om formål, rettar og lagringstid for opplysningane.

1.2 Informasjonstryggleik handlar om:

- Konfidensialitet
  - informasjonen er berre tilgjengeleg for dei som har behov for det i jobben sin
- Integritet
  - informasjonen er fullstendig, nøyaktig og gyldig, og er ikkje endra av uvedkomande
- Tilgjengelighet
  - informasjonen er tilgjengeleg til rett tid for dei som har behov for det

1.3 Kven gjeld informasjonstryggleikshandboka for?

Informasjonstryggleikshandboka er fastsett av rådmannen, og gjeld for alle som skal ha tilgang til Tysnes kommune sitt IT-system. Føresegnene i handboka gjeld for all behandling av informasjon i kommunen, både intern informasjon, offentleg informasjon, informasjon halde unna offentleg innsyn eller personopplysningar - under dette sensitive personopplysningar.

1.4 Kvifor treng me denne handboka?

I Tysnes kommune skal me verna informasjonen og informasjonssystema slik at informasjon ikkje kjem på avvegar. Me skal sikra at behandlinga av innbyggjarinformasjon oppfyller lovpålagde krav, kontraktsmessige forpliktingar og dekkjer behovet for personvern og etisk ansvar.

Informasjonstryggleikshandboka skildrar reglar og retningslinjer for behandling av informasjon for å vareta informasjonstryggleik og personvernet til samarbeidspartar, innbyggjarar, tilsette og elevar.

Det skal utarbeidast og takast i bruk rutineskildringar for behandling av informasjon i system og på fagområde, som er i samsvar med gjeldande lovverk. Alle som nyttar systema til kommunen er forplikta til å kjenna til og følgja informasjonstryggleiks-handboka.

1.5 Sikkerhetsstrategi

Val og prioriteringar for å sikra personopplysningar og behandling av desse.

- Arbeidet med informasjonstryggleik skal forankrast i øvste leiing og inngå i ansvarsområdet til vedkomande leiar
- Tilgang til system og informasjon blir gjeve til tilsette etter arbeidsrelaterte behov
- Det skal gjevast opplæring og informasjon til tilsette som brukar datasystemet til kommunen, for å sikra at gjeldande sikkerhetskrav blir ivareteke
- Uvedkomande skal hindrast tilgang til system og informasjon
- Det skal sikrast at personopplysningar ikkje blir forandra utilsikta eller uautorisert
- Det skal vera mogleg å spora uønskte hendingar knytt til bruk av datasystemet til kommunen
- Fysisk sikring skal hindra at uautoriserte får tilgang til lokale der personopplysningar blir behandla og lagra

- Det er rutinar og prosessar for å handtera uønskte hendingar, og avvik blir rapportert i f.t. Compilo
- Det skal gjennomførast tilfredsstillande internkontroll, under dette sikkerhetsrevisjonar og den årlege gjennomgangen til leiinga.

2. Informasjonstryggleik for alle tilsette

2.1 Tilgang og brukarkontroll

A. Alle tilsette får tildelt brukarnamn og passord for å autentisera den tilsette og gje tilgang til Tysnes kommune sitt IT-utstyr, system og nettverk.
B. Passordet skal haldast hemmeleg for andre, og det skal lærast utanåt. Passordet skal som hovudregel ikkje skrivast ned. Dersom det likevel må skrivast ned, må det gjerast på ein slik måte og på ein slik stad at ikkje andre kan få tilgang til det. Det er ikkje tillate å bruka/låna brukarnamnet og passordet til andre brukarar.
C. Bruk andre passord i systema til kommunen enn dei du brukar på private innloggingar.
D. Dersom tilsette har gløymt passordet, eller mistenkjer at passordet har vorte kjent for andre, skal den tilsette kontakta IT eller bruka iforgot.tysnes.kommune.no for å få endra passordet omgåande.
E. Tilsette, konsulentar, vikarar og andre som skal ha tilgang til IT-systema skal ha underteikna erklæring om taushetsplikt.
F. Når tilsette forlèt PC-en, nettbrett, mobiltelefon m.m. skal denne låsast.

2.2 Lagring og behandling av data

Informasjon som blir lagra på løysingane til kommunen skal vera jobbrelatert. Dersom personopplysningar blir behandla i løysinga, skal det førast behandlingsprotokoll etter GDPR-reglar. Kontakt personvernombod for meir informasjon.

Før løysingar blir tekne i bruk skal det gjennomførast ein Ros-analyse.

2.3 Bruk av IT-utstyr, programvare og nettverk

Tilsette skal følgja kommunen sine retningslinjer om bruk av program, utstyr og tenester knytt til utstyret. Tilsette skal rapportera forhold som kan ha noko å seia for tryggleiken i IT-utstyret til IT avdeling så raskt som mogleg.

2.4 Bruk av elektronisk kommunikasjon (mobile einingar)

Med elektronisk kommunikasjon siktar ein til mobile einingar til bruk for internett-tilknyting (eks. nettbrett, mobiltelefonar). Elektronisk kommunikasjon blir brukt der tilsette har behov for tilgjengelegheit, beredskap, fleksibilitet og dessutan at det er eit verktøy i arbeidskvardagen. Sjå pkt. 2.3 vedkomande bruken av dette.

2.5 Ansvaret til den enkelte ved avslutning av arbeidsforhold

Den enkelte tilsette har ansvar for at det vert rydda opp i it-utstyr, mapper, filer, e-post-system o.s.v. før vedkomande sluttar.

3 Informasjonstryggleik for leiarar

3.1 Tilgang og brukarkontroll

Leiaren er ansvarleg for at tilsette har underteikna tilsetjingskontrakt og erklæring om teieplikt før dei får tilgang til IT- og fagsystema.

Leiaren skal sørgja for at tilsette i verksemda si er registrert i HR-systemet til kommunen, innmeldt til IT slik at den tilsette kan få delt ut brukarnamn og passord og tilgang til kommunen sitt IT-utstyr, fagsystem og nettverk.

Leiaren er ansvarleg for at tilgangen til tilsette i system og program er avgrensa til berre det dei har behov for i arbeidet.

Leiaren er ansvarleg for å gi rett tilgang til lokala i eininga.

Når tilsette sluttar skal leiar syta for at tilgang til nettverk, system og data stansar, jf rutiner om avslutning av arbeidsforhold vedteke av kommunestyret.

3.2 Lagring og behandling av data

Leiar har ansvar for å leggja til rette for at tilsette lagrar og behandlar opplysningar på rett stad i fagsystema, på heime- eller fellesområdet eller i Teams for kommunen. Leiar har ansvar for at formålet med behandling av data skal registrerast i samsvar med GDPR reglane. Det skal utarbeidast Ros analysar ved nye system eller større endringar i eit fagsystem.

3.3 Sensitive opplysningar

Leiar må ha informasjonstryggleik som fast punkt på møte i verksemda.

3.4 Innkjøp av IT-utstyr og programvare/lisensar

Programvare og utstyr skal skaffast etter gjeldande reglar for innkjøp.

IT og personvernombod skal alltid involverast ved innkjøp av nye programvareløysingar.

IT skal alltid involverast ved kjøp av IT-utstyr.

3.5 Opplæring

Tilsette skal ha tilstrekkeleg opplæring i dei systema som skal nyttast. Dette omfattar:

- grunnleggjande kompetanse i kontorstøtteverktøy
- å kunna følgja retningslinjer for kor informasjonen blir lagra, blir brukt og delt
- opplæring i aktuelle fagprogram og rutinar knytt til bruken av system
- kunnskap om innhaldet i informasjonstryggleikshandboka

3.6 Når tilsette sluttar

- Leiar er ansvarleg for å melda frå til personal, IT og superbrukar for aktuelle fagsystem.
- Leiar er ansvarleg for innsamling av nøklar og ID-kort.

3.7 Avvik

Alle tilsette skal ha kjennskap til korleis avvik skal registrerast i avvikssystemet til kommunen - Compilo. Dette skal gjerast med ein gong etter at avviket er oppdaga.

Organisering og ansvar

- Rådmann
- Rådmannen si leiargruppe
- IT-leiar
- Personvernombod
- Einingsleiarar
- Alle tilsette

Linjeleiinga har ansvaret for at informasjonstryggleikshandboka vert følgd.

3.8 Roller

Alle tilsette i Tysnes kommune skal overhalda informasjonstryggleiks-reglementet, og vera med på å verna verdien som ligg av informasjon i fagsystem, elektroniske einingar og infrastruktur.

Personvernombod

Personvernombod skal hjelpa tilsette, registrerte og leiinga i spørsmål om personvern og informasjonstryggleik. Personvernombod har teieplikt, skal ikkje få instruksjonar i samband med utføring av oppgåvene som personvernombod, og rapporterer til rådmannen.

Personvernombod kontrollerer etterleving av forordninga og skal kunna gje råd i personvernkonsekvensutgreiingar og kontrollera gjennomføringa.

Alle tilsette som oppdagar eit brot på informasjonstryggleika og brot på reglementet, skal varsla om dette til personvernrombod, og på den måten hjelpa til med å avgrensa eller hindra at opplysningar kjem på avvegar, blir urettmessig endra eller forsvinn.

Leiarar

Den enkelte leiar har det daglege ansvaret for den praktiske oppfølginga av sikkerhetsarbeidet i eiga verksemd. Leiar er også ansvarleg for å initiera og hjelpa til i risikovurderingar.

Behandlingsansvarleg

Rådmannen har hovudansvaret for behandling av personopplysningar i Tysnes kommune. Det daglege ansvaret er delegert til einingsleiar for den aktuelle behandlinga. Delegeringa omfattar berre oppgåvene, ikkje ansvaret.

Einingsleiar er ansvarleg for å behandla personopplysningar på ein lovleg, rettferdig og gjennomsiktig måte, ha eit behandlingsgrunnlag, behandla personopplysningane på ein sikker måte og sikra at dei registrerte får utøvd rettane sine.

Einingsleiar må syta for å etablera alle nødvendige organisatoriske og tekniske tiltak for å sikra at regelverket til kvar tid blir etterlevd. Einingsleiar må kunna visa at han opptrer i samsvar med reglane. Dette gjeld også med omsyn til forsvarleg val av databehandlar. Einingsleiar kan med andre ord ikkje seia frå seg ansvaret for å etterleva regelverket fordi sjølve behandlinga av personopplysningane skjer hos ei anna verksemd.

Elevar

Elever er brukarar av Tysnes kommunes IT-system, og det er ansvaret til skulen å syta for informasjonstryggleika til elevane.

IT og digitalisering

IT-leiar er ansvarleg for at informasjonstryggleika blir vareteken i infrastruktur, maskinvare og sikkerhetssystem.

IT-leiar ivaretek sentral beredskapsplan for å handtera driftsavbrot som blir vurdert å vera av eit slikt omfang at dei skaper vesentlege forstyrringar for større delar av kommuneverksemda, og/eller som kan gi følgjeskadar for tredjepart.

Systemeigar

Einingsleiar er systemeigar, og er eigar av fagsystema/IT-systema som naturleg høyrer inn under området einingsleiar er ansvarleg for. Systemeigar er ansvarleg for å vareta informasjonstryggleik i fagsystema/IT-systema. Einingsleiar utnemner ein person for dagleg ivaretaking av superbrukar/-fagsystemansvarleg rolla.

Superbrukar/fagsystemansvarleg

Superbruker/fagsystemansvarleg er utpeika av einingsleiar. Dei har hovudansvar for å gi opplæring til tilsette av fagsystema/IT-systema om forsvarleg forvaltning av informasjonen. Dei har også ansvar å utarbeida risikoanalyse.

Systemansvarleg

IT-leiar er ansvarleg for at fagsystema/IT-systema er tilgjengeleg for tilsette. IT-leiar vil hjelpa til med teknisk kompetanse ved vidareutvikling i dialog med superbrukar/fagsystemansvarleg.

Leverandør/partnar

Informasjonstryggleik blir regulert i kontrakt og databehandlaravtale mellom leverandørar og kommunen. Det skal inngåast databehandlaravtale med

leverandørar/firma/partnar som behandlar personopplysningar. Kommunen skal alltid ha rett til innsyn og måling av om sikkerhetskrav blir følgd av leverandør eller eksterne tilsette.

Det skal inngåast databehandlaravtale med leverandørar/firma/partnar som behandlar personopplysningar. Alle databehandlaravtalar blir arkiverte i kommunen sitt arkivsystem.

Innkjøp av nytt IT-system

I innkjøpsprosessen skal det bli stilt krav om innebygd personvern og personvern som standardinnstilling. Det er viktig å sikra at personopplysningar ikkje kjem på avvegar, derfor må det stillast krav til løysingar der personvern har høg prioritet.

Det skal utnemnast ein systemeigar som er behandlingsansvarleg for systemet og har ansvaret for at oppgåvene rundt forvaltninga og risikoanalyse. Systemeigaren rådfører seg med IT-leiar og personvernombod i alle spørsmål knytt til personvern og behandling av personopplysningar.

Systemeigar saman med IT-leiar er ansvarleg for å gjennomføra ROŠ analyse der formålet med behandlinga av behandlinga til systemet av personopplysningar blir gjennomførte og personopplysningane blir gjort greie for. Det skal alltid vurderast om ein DPIA skal utarbeidast.

Forvaltning av IT-systemet

Det skal gjennomførast årleg gjennomgang av informasjonstryggleik med oppdatering av risikovurderinga. Det er systemeigar som er ansvarleg for gjennomføring av årleg informasjonstryggleiksgjennomgang, saman med personvernrådgivar og IT-leiar.

Databehandlaravtalar skal gåast gjennom og fornyast ved behov.

Avhending av IT-system

Når eit IT-system ikkje lenger skal brukast, skal data som ligg i systemet bli sikra med omsyn til konfidensialitet, integritet og tilgjengelegheit. Informasjonen skal arkiverast i samsvar med lovverket, og det skal vera mogleg å føra vidare bruk av registrerte data i andre system.

Systemeigar er ansvarleg for at informasjonen blir ivareteken på ein sikker måte når systemet ikkje lenger skal brukast. Arkivtenesta hjelper saman med systemeigar for å sikra rett forvaring.

4 Internkontroll

4.1 Behandling av avvik

Formålet med avviksbehandlinga er å få kunnskap om hendingar slik at kommunen kan avgrensa skadane, læra av hendingane og endra rutinar og implementera gode løysingar. Dette for å hindra at liknande hendingar skjer igjen, i tillegg til å sikra at me til ei kvar tid varetek innbyggjarane våre sitt personvern.

Hendingar som skal meldast som avvik kan vera enkeltepisodar, gjentakande episodar, regelbrot, svikt i rutinar, funksjonsfeil i fagsystemet eller liknande, der personopplysningar har komme på avvegar, ikkje lenger er korrekte eller oppdaterte, eller har gått tapt. Også personopplysningar som er krypterte kan gå tapt eller komma på avvegar, og dei skal også meldast til datatilsynet. Det er viktig at dei registrerte også får beskjed så tidleg som mogleg slik at dei kan gjera nødvendige tiltak.

Alle som oppdagar eit avvik, har ansvar for å melda dette i avvikssystemet Compilo. Alvorlege brot vil bli varsla vidare til personvernombod.

Mottak og behandling av avviksmelding

Personvernombod kan få avviksmeldinga som ein munnleg førespurnad, tekstmelding, telefon eller som eit avviksmeldingsskjema. Ei melding om avvik til personvernombodet skjer fortruleg, og personvernombodet har teieplikt og varetek anonymiteten til meldaren. Personvernombodet vil også kunna setja i gang avviksbehandling på eige initiativ, utan at ei formell avviksmelding er motteken.

- Avvik blir registrert i Compilo. Dersom avviket er av ein slik karakter at det er fare for at personopplysningar har komme på avvegar, vorte urettmessig endra eller gått tapt, skal avviket meldast datatilsynet
- Følg instruksane i Compilo for melding til datatilsynet.
- På bakgrunn av opplysningar i avviksmelding, vil personvernombodet kontakta aktuelle ressursar, f. eks systemansvarleg, behandlar eller leiar for å avklara realiteten i og omfang av avviket, og vera med og finna forslag til tiltak for å lukka avviket og avgrensa skaden
- Personvernombodet, IT-leiar, behandlingsansvarleg og systemeigar vurderer omfanget av avviket, alvorsgrad og allereie i gangsette tiltak.
    - Har personopplysningar kome på avvegar, vorte urettmessig endra eller sletta slik at Datatilsynet skal varslast?
    - Har det allereie vorte sett i gang tilstrekkeleg gode tiltak for å lukka avviket og hindra nye avvik - kan avvikssaka lukkast?
    - Ved behov kontaktar personvernombodet Datatilsynet om spørsmål ved hendinga.
- Personvernombodet formar ut og sender melding til dei registrerte på vegner av behandlingsansvarleg og systemeigaren i dei tilfella der personopplysningar har komme på avvegar, vorte urettmessig endra eller gått

tapt. Meldinga til dei registrerte blir signert av behandlingsansvarleg og skal sendast utan ugrunna opphald. Den kan vera i form av e-post, pressemelding eller anna skriftleg melding som vil nå alle ramma.

- Dokumentbehandlinga skal skje i saksmappa i sak/arkivsystemet, der dei i utgangspunktet vert unnatekne offentleghet.
- Personvernombodet utformar notat for avvikssaka. Ved avvik der tilstrekkelege tiltak for å lukka og hindra nye avvik er sett i gang, kan avvikssaka foreslåast lukka. Avviksmelding til Datatilsynet og melding til dei registrerte blir lagd ved der dette er aktuelt. Notatet med vedlegg blir sendt til behandlingsansvarleg som vedtek om avvikssaka kan lukkast.

Notatet for avvikssaka skal innehalda:

- Orientering om saka
- Skildring av hendinga, når hendinga vart oppdaga, når hendinga skjedde, kven som var involverte og andre relevante opplysningar om hendinga
- Reglar og retningslinjer som ligg til grunn for saka
- Drøfting av saka
- Vurdering av avviket, forslag til tiltak og vurdering av foreslegne tiltak for å lukka avviket og hindra nye avvik
- Konklusjon med eventuelle oppfølgingspunkt

Meldinga til Datatilsynet skal innehalda:

- Skildring av brot på personvernet, kva slags brot det er og kor mange registrerte som er ramma
- Kontaktopplysningar på personvernombodet eller ein annan kontaktperson ved varsling til datatilsynet
- Skildring av moglege konsekvensar
- Skildring av iverksette tiltak og tiltak som er planlagde sett i verk mot personvernbrotet. Der det er aktuelt, informasjon om tiltak for å hindra moglege uheldige verknader av tiltaka
- Brot på personvernet skal dokumenterast. Dokumentasjonen skal innehalda fakta om brotet, konsekvensane og tiltaka som er gjorde for å avgrensa skaden. Dokumentasjonen skal verifisera at pålegg er følgt
- Kontaktopplysningar til personvernombodet om det er behov for utfyllande opplysningar
- Ved brot på personvernet skal dei(n) registrerte blir varsla utan ugrunna opphald av behandlingsansvarlege

Meldinga til dei registrerte skal innehalda:

- Skildring av brot på personvernet
- Skildring av moglege konsekvensar
- Skildring av iverksette tiltak og tiltak som er planlagde sett i verk mot personvernbrotet. Der det er aktuelt, beskriv tiltak for å hindra moglege uheldige konsekvensar av tiltaka

- Eventuell skildring av tiltak den registrerte blir tilrådd å gjera
- Kontaktopplysningar på personvernombodet og leiar/systemeigar eller ein annan kontaktperson

4.2 Loggføring

For å sikra integritet og sporbarhet skal all aktivitet i fagsystem som behandlar personinformasjon bli loggførte, slik som endring og sletting av opplysningar, men også søk etter opplysningar.

4.3 Innsyn

Fellestenesta kan kontaktast ved innsynskrav.

4.4 Gjennomgang av informasjonstryggleik for leiargruppa

Gjennomgangen til leiinga skal haldast årleg for leiargruppa til rådmannen. I møte skal det samanfattast status for informasjonstryggleiksarbeidet i kommunen, og dessutan avdekkast om tryggleiken blir vareteken i høve mål, strategiar og prosedyrar og vedtakast tiltak for det vidare sikkerhetsarbeidet. Tiltak skal sikra at sikkerhetsmål, strategi og organisering av informasjonstryggleikssystemet er oppdaterte og i samsvar med behovet til kommunen.

I gjennomgangen til leiinga skal m.a. følgjande punkt gåast gjennom og bli vurderte:

- Resultat og hovudkonklusjonar frå informasjonstryggleiksrevisjonar
- Registrerte avvik
- Rapporter frå offentlege og interne tilsyn
- Endringar i lover, forskrifter og offentlege sikkerhetskrav
- Endringar i dei personopplysningane som verksemda skal behandla
- Endringar i trusselbiletet som kjem fram i gjennomførte risikovurderingar
- Status på hendingar rundt teknisk informasjonstryggleik
- Organisatoriske endringar
- Bygningsmessige endringar
- Planar og framdrift for å ivareta intern kontroll og informasjonstryggleik

4.5 Overvaking

Kameraovervaking

Kameraovervaking skal ha som formål å hindra at uvedkomande skaffar seg tilgang til områda for verksemda, og skal verka preventivt på uønskte hendingar som tjuveri, innbrot, vald, hærverk osb. Kameraovervaking av personar som kan kjennast igjen, er eit inngrep i personvernet. Difor skal det gjennomførast ei vurdering av personvernkonsekvensar ved systematisk overvaking i stor skala av eit offentleg tilgjengeleg område. Kameraovervaking skal ikkje finna stad dersom problemet kan løysast eller risikoen blir minimert gjennom alternative tiltak. Kameraovervaking skal vera sakleg grunngjeve ut frå formålet sitt i verksemda, og skal utøvast i samsvar med føresegnene i personopplysningslova.

Behandlingsansvarleg skal ivareta det overordna ansvaret for kameraovervaking ved einingane. Det løpande ansvaret for oppfylling av pliktene til den behandlings-ansvarlege blir ivareteke av kvar enkelt einingssleiar.

Personopplysningar skal lagrast slik at dei blir sletta eller blir anonymiserte når dei ikkje lengre er nødvendige for formålet dei vart innhenta for.

Lydopptak

Lydopptak kan gjerast der formålet er å sikra dokumentasjon for ei eventuell politisak og dessutan for å ivareta eit HMS-perspektiv, og der formålet er å sikra dokumentasjon for dei merknadene som blir sett fram, og dessutan kva som er lova av respons.

Innringjar blir varsla om at opptak blir gjort når opptaket startar dersom ikkje det i seg sjølv blir vurdert som ein risiko.

- Når innringjar blir oppfatta som truande eller set fram konkrete truslar.
- Når innringjar set fram ei klage og ikkje vil snakka med saksbehandlar, eller saksbehandlar ikkje er tilgjengeleg. Det bør lagast eit notat til saksbehandlar i kommunens sak- og arkivsystem på den aktuelle saka.

Oppbevaring og sletting

Kameraopptak og lydopptak kan innehalda sensitive personopplysningar og skal oppbevarast slik at informasjonstryggleika og personvernet blir ivareteke. Opptak skal slettast når det ikkje lenger er sakleg grunn for oppbevaring. Sletteplikta gjeld likevel ikkje dersom det er sannsynleg at opptaket vil bli utlevert til politiet i samband med etterforsking av straffbare handlingar eller ulukker.

4.6 ID-kort

ID-kort vert brukt som nøkkelkort i dei bygg som har slik låssystem. Tap av kort må meldast til leiar og til fellestenesta. Tapt kort må slettast snarast og nytt kort bestillast.

4.7 Avhending av datautstyr

Utrangert datautstyr kan leverast til IT, som syt for at harddisk og liknande vert levert til destruksjon på sikker måte.