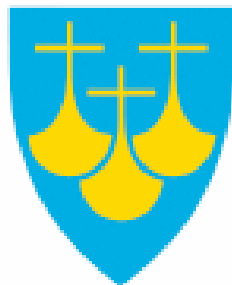


---

# Handbok i informasjonstryggleik

## Møre og Romsdal fylkeskommune

Versjon 02 mars 2010



Møre og Romsdal  
fylkeskommune

---

## Forord

Møre og Romsdal fylkeskommune er ein viktig produsent av tenester innan område som t.d. utdanning, samferdsel, næringspolitikk, kultur og tannhelse. Informasjonsteknologien er blitt stadig meir sentral i denne produksjonen. For dei fleste medarbeidarane i fylket er datamaskin og nettverk det desidert mest sentrale verktøyet.

Det er viktig at dei datamengdene og den informasjonen vi samlar inn, nyttar og produserer blir handtert så trygt og sikkert som råd. Det er derfor laga verktøy og rammeverk for korleis personopplysningar blir behandla i organisasjonen og kva som blir gjort for at informasjon blir verna mot uautorisert innsyn, er tilgjengeleg for dei som skal ha tilgang til den, ikkje skal gå tapt eller bli utilsikta endra eller forvrengt.

Denne handboka er eit verktøy for dei som har tryggleiksansvar og IT-driftsansvar i organisasjonen. Dei som er involvert i informasjonstryggleik skal bruke handboka som ein første referanse for korleis tryggleiksansvaret skal handterast. Det er viktig at verksemdene veit kven som gjer kva når det gjeld å halde oppe ei så god informasjonsforvaltning som råd.

Dokumentet inneheld dei viktigaste måla og korleis tryggleiksarbeidet er organisert. Du vil også finne nokre malar for rapportering og verktøy for til dømes risikovurdering.

Arbeidet med informasjonstryggleik er eit kontinuerleg arbeid. Det er ikkje eit arbeidsstykke som blir utført ein gong kvart år – det gjeld berre hovudrevisjonen. Dei viktigaste aktivitetane innan tryggleiksarbeid er den løpande risikovurderinga og behandling av avvik. Arbeid med informasjonstryggleik er basert på at alle nye tiltak eller endring av eksisterande rutiner m.v. blir vurdert ut frå om personopplysningar kan komme på avvegar, eller om ein blir utsett for nye typar risiko-moment.

Når eit avvik blir oppdaga er det viktig at det om mogleg i avdelinga/skulen m.v. blir lukka straks og rapportert til overordna tryggleiksansvarleg slik at ein og kan få kontrollert om det er eit gjennomgåande avvik i organisasjonen.

Det viktigaste elementet i tryggleiksarbeidet er haldningane til medarbeidarane. Alle har plikt til å melde frå om ting dei ser ikkje er i samsvar med god IT-tryggleik. Dette gjeld risiko-faktorar og avvik.

Vi er innforstått med at handboka slik ho no ligg føre nok vil ha manglar ved seg. Det er derfor særst viktig at alle som nyttar boks melder inn formuleringar, rutiner m.v. dei finn uklåre, upresise m.v.. På denne måten vil vi gjennom dei årlege revisjonar av handboka få eit stadig betre verkty i det viktige arbeidet med informasjonstryggleik.

Lukke til med det vidare arbeidet!

Ottar Brage Guttelvk  
Fylkesdirektør

---

## Innholdsliste

<a href="#">1. Bakgrunn og mål for handboka.....</a>	<a href="#">4</a>
<a href="#">2. Ansvar og organisering.....</a>	<a href="#">6</a>
<a href="#">3. Personopplysningar i datasystem .....</a>	<a href="#">8</a>
<a href="#">4. Risikovurdering, avviksbehandling og rapportering.....</a>	<a href="#">9</a>
<a href="#">4.1. Risikovurdering.....</a>	<a href="#">9</a>
<a href="#">4.2. Avviksbehandling og rapportering.....</a>	<a href="#">9</a>
<a href="#">5. Administrative og tekniske rutinar.....</a>	<a href="#">11</a>
<a href="#">6. Beredskapsplanlegging.....</a>	<a href="#">12</a>
<a href="#">7. Partnerar og leverandørar.....</a>	<a href="#">13</a>
<a href="#">8. Fysisk tryggleik.....</a>	<a href="#">14</a>
<a href="#">9. Kontroll og oppfølging .....</a>	<a href="#">15</a>
<a href="#">10. Vedlegg.....</a>	<a href="#">17</a>
<a href="#">10.1. Rammeverk for risikoanalyse.....</a>	<a href="#">17</a>
<a href="#">10.2. Mal for Risikovurdering.....</a>	<a href="#">19</a>
<a href="#">10.3. Mal for avviksrapportering.....</a>	<a href="#">20</a>
<a href="#">10.4. Avtale mellom skole/institusjon og ekstern partner.....</a>	<a href="#">21</a>
<a href="#">10.5. Rutine for tryggleikskopiering.....</a>	<a href="#">22</a>
<a href="#">10.6. Forslag til møteinnkalling for gjennomgang av informasjonstryggleiken med leing.....</a>	<a href="#">23</a>

---

## 1. Bakgrunn og mål for handboka

Handboka er eit overordna reiskap for IT-trygging i Møre og Romsdal fylkeskommune. Handboka omfattar ikkje berre IT-trygging, men også behandling og oppbevaring av sensitive dokument i papirform og manuelle register som inneheld personopplysningar.

Handboka byggjer på:

1. Lov om personopplysningar (<http://www.lovdatab.no/cgi-wift/wiftldrens?/usr/www/lovdatab/ltavd1/filer/nl-20000414-031.html>)
2. Kapittel 2 i føresegnene til personopplysningslova (<http://www.lovdatab.no/cgi-wift/wiftldrens?/usr/www/lovdatab/for/sf/fa/xa-20001215-1265.html>)
3. Veiledning i informasjonssikkerhet for kommuner og fylker (<http://www.lovdatab.no/cgi-wift/wiftldrens?/usr/www/lovdatab/for/sf/fa/xa-20001215-1265.html>) utgitt av Datatilsynet.

Tryggleiksutvalet reviderer handboka årleg. Handboka skal sikre at personvernet ikkje blir krenka gjennom behandlinga av personopplysningar. Handboka legg til rette for eit internkontrollsystem for informasjonstryggleik.

### Mål

Møre og Romsdal fylkeskommune sitt mål for informasjonstryggleik, er:

- at opplysningar ikkje kjem uvedkomande i hende
- å sikre tilgjenge til opplysningane slik at dei med tenesteheimel kan bruke opplysningane når dei treng dei
- å sikre at personopplysningar er korrekte (ikkje blir utilsikta endra)

### Krav

- Dei mest alvorlege risikofaktorane skal følgjast opp med jamne mellomrom
- Kvar skole/verksemd skal ha oversikt over og reviderte lokale rutinar for handtering av ulike register, manuelle som elektroniske som inneheld personopplysningar
- Ingen personopplysningar skal kome u-autoriserte eller uvedkomande personar i hende. Systemegar må såleis kunne dokumentere kven som er autorisert til kva og kven som kan gi autorisasjon.

### Strategi for tryggleiksarbeidet

Gjennom kontroll og oppfølging basert på lov, forskrift og retningslinjene gitt m.a. av Datatilsynet vil det bli gjennomført periodiske revisjonar av organisering, driftsrutine og retningslinjer.

Risikoanalyse, driftsovervaking og avviksoppfølging, vil danne grunnlag for justering av sikringstiltak.

Verksemda sin strategi for sikring av informasjonssystem med personopplysningar føreset at :

- 
- leinga i kvar einskild verksemd og avdeling har ansvar for og set i verk alle adekvate tiltak for sikring av informasjonssystema
  - organisering som vedkjem bruk og sikring av informasjonssystem er eintydig og dokumentert
  - bruk av eksterne partar kor personopplysningar kan eksponerast skal vere regulert av avtalar som også omhandlar informasjonstryggleik
  - sikring av informasjonssystema kviler på tiltak av ulik art, der det viktigaste er :
    - at personalet som har tilgang til tenesteheimla informasjon, har kompetanse til å bruke systemet/informasjonen, og er lojale mot sikringsregimet
    - at systemberande utstyr og sikringsbarrierar er fysisk sikra
    - at sensitiv personinformasjon berre blir behandla i ei sikra sone skilt frå intern sone med intern sikringsbarriere (sjå kapittel 11.)

---

## 2. Ansvar og organisering

Kravet til leiinga er sett i føresegnene til personopplysningslova (<http://www.lovdata.no/for/sf/fa/ta-20001215-1265-002.html#2-3>).

### § 2-3. Sikkerhetsledelse

”Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapitlet 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.”

Fylkesdirektøren er Møre og Romsdal fylkeskommune sin behandlingsansvarlege.

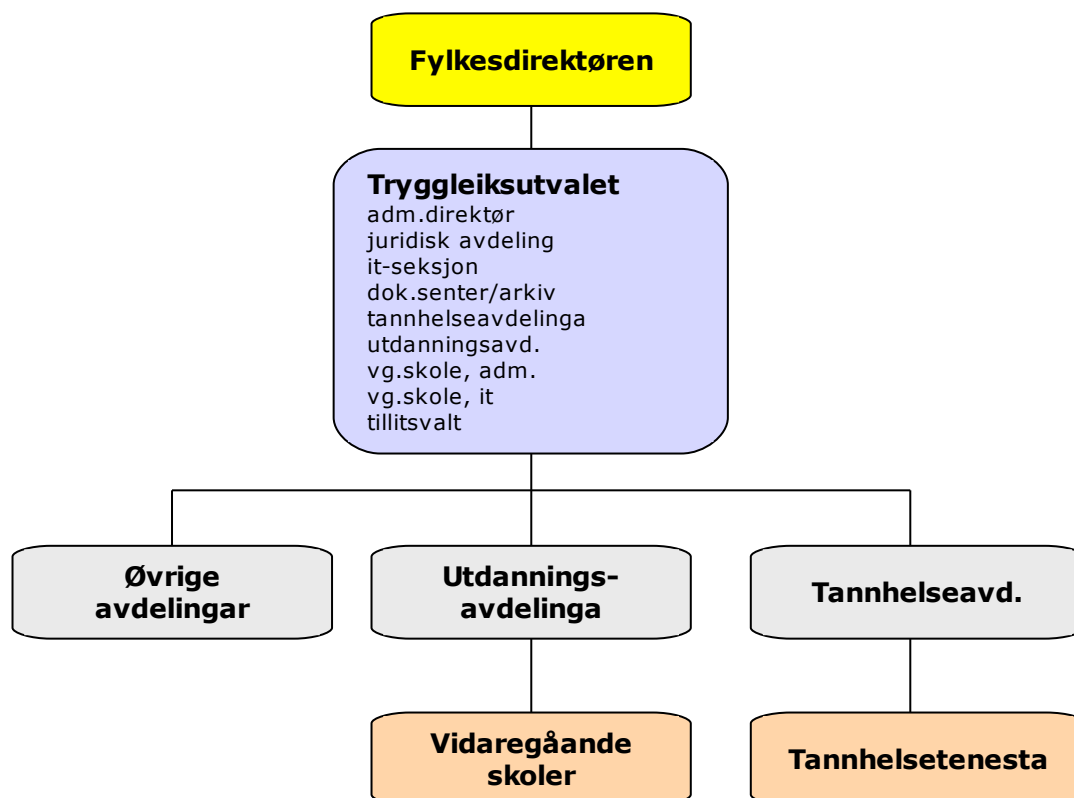
Behandlingsansvarleg er den som bestemmer formålet med behandlinga av personopplysningar og dei hjelpemiddel som skal brukast.

Leiinga ved kvar avdeling (kalt tryggleiksansvarleg) har det løpande ansvar for at verksemda sine personopplysningar er tilfredsstillande sikra.

Tryggleiksansvarleg har ansvar for å setje i verk og dokumentere tiltak som skal sikre personvernet, kompetansen og organiseringa (ansvar og oppgåvefordeling).

For å ivareta fylkesdirektøren sine oppgåver etter lova har fylkesdirektøren sett ned eit tryggleiksutval. Utvalet er leia av juridisk sjef. I tillegg består det av:

- administrasjonsdirektør, leiar for IT - seksjonen og leiar for dokumentresenteret
- 3 representantar frå utdanningsavdelinga
- 1 representant frå tannhelseavdelinga
- 1 representant frå tillitsvalde



### 3. Personopplysningar i datasystem

Overordna informasjon om kvart system som inneheld personopplysningar går fram av tabellen under. Detaljert informasjon om handtering av personopplysningane skal gå fram av eigne prosedyrar frå systemeigarane.

Dei behandlingsansvarlege si meldeplikt er regulert i personopplysningslova § 31. Meldeplikta inneber at den som ønskjer å bruke personopplysningar, skal orientere Datatilsynet før behandlinga blir starta.

Informasjon, formål	System	Heimel	Klassifisering	Sikrings-tiltak	Lagring og kommunika-sjon	Register omfang	Konsesjon og arkivering	Systemeigar
Løn og personal	Visma Unique	Lov om personoppl. § 8, § 9, første ledd, jfr. AML § 20	Person-opplysningar	Lukka nett eigen prosedyre	Database hos EMS-Infomedica Fast fibersamband	ca. 3000	Ingen konsesjonsplikt, men meldeplikt	Adm. Avd
Tannlege-system	Opus	Lov om personoppl. § 9, første ledd, jfr. lov om helsepersonell § 39,	Sensitive opplysningar	Sikker sone	Eigen server	75.000 - 100.000 pasientar	Ingen konsesjonsplikt, men meldeplikt	Tannhelse - avdelinga
E-læring	Class fronter	Lov om personoppl. § 8, § 9, første ledd, jfr. AML § 20, og l.vgo.	Person-opplysningar	Adgangs-kontroll via brukarnamn og passord	Internett teneste	9500 elevar 1750 tilsette		Utd. avd. o
Elev-inntak	Vigo	Lov om personoppl. § 8, § 9, jfr. l.vgo.	Person-opplysningar	Lukka nett	Eigen server	11.000 søkjarar	Ingen konsesjonsplikt, men meldeplikt	Utd. avd.
OT-ungdom	Otto	Lov om personoppl. § 8, § 9, jfr. l.vgo.	Person-opplysningar	Lukka nett	Eigen server	ca 2500	Ingen konsesjonsplikt	Utd. avd
Lærlinge-bedrifter - lærlingar	Vigo	Lov om personoppl. § 8, § 9, første ledd, jfr. l.vgo.	Person-opplysningar	Lukka nett	Eigen server	775 lærlingar	Ingen konsesjonsplikt, men meldeplikt	Utd. avd.
Skole-adm. register Tilsette og elevar ved skolar	Extence	Lov om personoppl. § 8, § 9, første ledd, jfr. AML § 20, og l.vgo.	Person-opplysningar	Lukka nett	Sentral server via faste ISDN-samband og fiber/trådløst samband	9500 elevar 1750 tilsette	Ingen konsesjonsplikt, men meldeplikt	Utd. avd.
Fraværs-registrering i VGS	Skole - arena	Lov om personoppl. § 8, § 9, første ledd, jfr. l.vgo.	Person-opplysningar	Adgangs-kontroll via brukarnamn og passord	Internett teneste	9500 elevar 1750 tilsette	Ingen konsesjonsplikt, men meldeplikt	Utd. avd.
Gruppevare - system	Lotus Notes	Lov om personoppl. § 8, § 9, første ledd, jfr. AML § 20	Person-opplysningar		Eigen server	1500 adresser	Ingen konsesjonsplikt	IT-seksjonen
Sak/arkiv-system	Ephorte	Lov om personoppl. § 8, § 9, første ledd, jfr. arbeidsm.l. § 20	Saksopp-lysningar som kan vere knytta til personar	System-funksjonar som sperrer mot innsyn	Eigen server	Personal-saker, jur. saker etc. varierende omfang	Ingen konsesjonsplikt, men meldeplikt	Adm. avdelinga

---

## 4. Risikovurdering, avviksbehandling og rapportering

### 4.1. Risikovurdering

Risikovurdering skal gjennomførast før behandling av personopplysningar blir sett i gang. Resultatet av risikovurderinga skal dokumenterast.

Risikoanalyse skal gjennomførast ved:

- innføring av nye informasjonssystem
- endringar av betydning for informasjonstryggleik

Det er leiinga som er ansvarleg for at det blir gjennomført risikovurderingar.

I si enklaste form kan dette gjerast ved at ein set opp potensielle hendingar. Deretter vurderer ein:

- risiko for at kvar hending kan inntreffe (sannsyn)
- konsekvensar dersom hendinga skulle inntreffe

Sjå vedlegg 10.1

### 4.2. Avviksbehandling og rapportering

Forskrifta til personopplysningslova seier i § 2-6:

*”Bruk av informasjonssystem som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik. Avviksbehandlinga skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.*

*Dersom avviket har medført uautorisert utlevering av personopplysningar hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.*

*Resultat fra avviksbehandling skal dokumenteres.”*

Det skal skrivast ein avviksrapport når:

- tilsette brukar informasjonssystem(a) utan autorisasjon og/eller fastsett opplæring
- virus har komme gjennom virusvernet og gjort skade/spreidd seg
- utilsikta utlevering av personopplysningar har funne stad
- informasjonssystem(a) blir utsett for innbrot eller forsøk på innbrot
- utilsikta endring i personopplysningane har skjedd
- feil i utstyr og/eller program verkar inn på sikring av og bruk av informasjonssystem(a)

Denne lista er ikkje uttømmende.

---

Avviksrapporten skal:

- bruke skjemaet som er vedlegg i kapittel 10.3 som mal
- sendast til driftsansvarleg (e-post- eller word-mal)
- driftsansvarleg skal sette i gong dokumenterte, korrigerande tiltak som skal leggst fram ved verksemda sin eigenkontroll

Dokumentasjon frå risikovurdering og avviksbehandling skal behandlast og arkiverast lokalt.

Dersom det blir oppdaga alvorlege avvik eller ein risikofaktor som kan få kritiske/katastrofale følgjer og blir vurdert som sannsynleg, skal dette rapporterast direkte til tryggleiksansvarleg hos fylkesdirektøren.

---

## 5. Administrative og tekniske rutinar

Informasjonssystema skal brukast i samsvar med fastlagde rutinar. I den grad det er behov for rutinar for å oppnå tilfredsstillande informasjonstryggleik, skal desse utarbeidast for bruk, drift og vedlikehald av utstyr og program. Systemeigar er ansvarleg for at desse rutinane finst.

Tryggleiksansvarleg har ansvar for å etablere og vedlikehalde rutinar for sitt område. Rutinane skal leggst til grunn ved eigenkontroll. Personelltryggleik fokuserer på kompetansekrav, teieplikt og autorisasjon.

Tryggleiksansvarleg har ansvar for å:

- setje og kontrollere kompetansekrav
- gjennomføre teieplikrutine (arkivere signerte dokument)
- autorisere nytt personell eller personell med nye oppgåver

Tilsette skal ha kompetanse til å utføre tenesteheimla oppgåver. Dette krev at verksemda har rutinar for å utvikle kompetanse, og halde denne vedlike. Tryggleiksansvarleg har ansvar for å oppdatere kompetansen om tryggleikssystemet for leiarane.

Tryggleiksansvarleg har ansvar for at tilsette er kjent med kva informasjonstryggleik inneber og at tilsette skriv under teiepliktskjema. Dei tilsette skal vere orientert om teieplikta sitt omfang, og konsekvensar ved brot.

Leiinga har ansvar for å autorisere tilsette til å bruke informasjonssystem(a). Leiinga skal melde autorisasjonar til systemeigar for respektive system. Meldingar om autorisasjonar skal arkiverast i sentralt arkiv.

Det skal utarbeidast rutine for autorisasjonstildeling som omfattar:

- autorisasjon av nyttilsette, vikarar etc. i forhold til tenestleg behov
- behov for endring ved endring av oppgåve (sletting og endring av autorisasjonar når brukarane av systema sluttar, eventuelt endrar oppgåve)
- kontroll med at tildelt autorisasjon fungerer etter føresetnadene

Personalkontoret skal leggje fram lister over tilsette som har slutta i ein periode slik at IT-seksjonen / systemeigarar kan verifisere og tilbakekalle autorisasjonar.

Driftsansvarleg IT har ansvar for å:

- autorisere personell som skal ha tilkomst til spesielle område, soner etc.
- sikre dataoverføring
- dokumentere konfigurasjonar, oversikter, endringar etc.
- kontrollere loggar
- utarbeide utkast/dokument til risikovurderingar

## 6. Beredskapsplanlegging

Sidan meir og meir informasjon blir lagra elektronisk er verksemda avhengig av at informasjonen er tilgjengeleg til ei kvar tid.

Målet med beredskapsplanlegging er å planleggje tiltak for situasjonar med avbrot i normal drift for å gjenopprette normal tilstand.

Beredskapsplanlegging for informasjonssystema går inn i verksemda sitt rullerande arbeid med beredskaps- og kriseplanar.

Gjeldande praksis ved utilsikta stans i informasjonssystema:

Svikt	Reservesystem	Resultat	Vedkjem	Rutinar
Eksterne system	Hos leverandøren, kan kjøre ein del lokalt	Stans i e-læringssystem	Brukarane av e-læring systemet	Sjekk av eige nett, varsling til leverandør
Tele - og datasamband	Ikkje på samband, på eige ende-utstyr er det reserveløysingar	Stans i internett-trafikk. Ytre etatar mister tilgang på adm.systema.	Heile organisasjonen	Sjekk av eige nett, varsling til leverandør
Lokalt komm. utstyr	Reservemodular på dei mest kritiske komponentane	Mogleg stans i adm. system og fagsystem på delar av sentraladm	Avhengig av kva modul som sviktar	Setje inn reserve for defekt komponent
Lokal server	SAN-lagring	System ned inntil reserve-server er på plass	Avhengig av kva server/system som blir ramma	Rutinar for skifte av server

### Reservekopiering.

Fjern-backup blir gjort i eigen bygning.

Rutine for reservekopiering ligg som vedlegg i kapittel 10.5

---

## 7. Partnerar og leverandørar

I kontrakten med leverandørar skal det spesielt leggast vekt på:

- at leverandøren sitt personell er informert om den teieplikta som gjeld og at slikt personell skal underteikne teieplikterklæring
- å ha ei oversikt over personell hos leverandøren som skal ha tilgang til informasjonssystemet eller tilgang til område eller utstyr
- korleis verksemda si kontroll av tryggleik hos leverandør skal utførast

Sjå vedlegg i kapittel 10.4 for eksempel på kva vilkår som kan inngå i kontrakt mellom Møre og Romsdal fylkeskommune og leverandør.

Kontraktsvilkår blir fastsett av verksemda si leiing. Val av partnerar og leverandør, og inngåing av kontrakt kan bli utført av verksemda sin innkjøpsfunksjon, evt. av IT-ansvarleg.

---

## 8. Fysisk tryggleik

Fysiske tryggleikstiltak skal hindre at uvedkomande får tilgang til IKT -ressursar (informasjons- og kommunikasjonsressursar), tekniske installasjonar og sensitive personopplysningar. Det skal sikrast at slik tilgang er avgrensa til tilsette og partnerar med tenestleg behov.

Dei fleste lokala kan vere opne for besøk i kontortida, men besøkande skal aldri vere åleine.

### Tilkomst til område og utstyr

- Autorisering for tilkomst, sjå administrative og tekniske rutinar kap. 5
- Berre autorisert personale har tilgang til tele/datarom og leidningskanalar
- Tele/datarom og stigersjakter skal alltid vere låst for uautorisert personell
- Gjestar skal vere i følgje med autorisert personale (dvs. tilsette)
- Tele/datarom skal overvåkast for røyk, temperatur og fukt
- IT-utsyr på Tele/datarom og i stigersjakter skal koplast til UPS (batteri-backup) og evt. Nødstraumkursar

### Krav

- Tenarmaskiner, hovudsvitsj for nettverk ('nav i stjerne'), sikringsbarriere og ruter mot eksterne nett skal vere plassert på serverrom.
- Kantsvitsjar skal vere plassert i lag med andre tekniske installasjonar på etasjenivå (stigersjakter) på avlåste rom.
- Fellesskrivarar er plassert på eigne rom/ekspedisjonar.

### Skrivarar

Den som aktiviserer skrivaren med sensitive personopplysningar, plikter å gå til skrivaren og vente til utskrifta er ferdig og ta med seg alle utskrifter.

### Kopimaskin

Saksbehandlar må vente ved kopimaskina til alle dokument med sensitive personopplysningar er kopierte. Den som kopierer, plikter å sjå til at maskina er tømte for originalar og kopiar før han/ho forlet maskina.

### Kontor

Kontor der det blir behandla sensitive personopplysningar, skal låsast når autorisert personell ikkje har tilsyn med rommet. Dokument med sensitive personopplysningar skal lagrast nedlåst etter kontortid.

### Arkiv

Arkivet skal låsast ved arbeidsdagens slutt, og når arkivet ikkje er under tilsyn i arbeidstida.

---

## 9. Kontroll og oppfølging

Kontrollaktivitetar skal sikre at tryggleikssystema fungerer, og blir etterlevd. Målet er å sjekke ut at dei tiltaka som er sette i verk for å hindre avvik blir følgde.

Kontrollsystemet består av :

- Informasjonstryggleikshandboka – dette dokumentet med vedlegg
- Gjennomførande dokumentasjon – for eksempel rutinar og instruksar
- Kontrollerande dokumentasjon – sjekklister, eigenkontroll og rapportar (for eksempel risikoanalyse) for å sikre at eventuelle avvik blir oppdaga og blir lukka

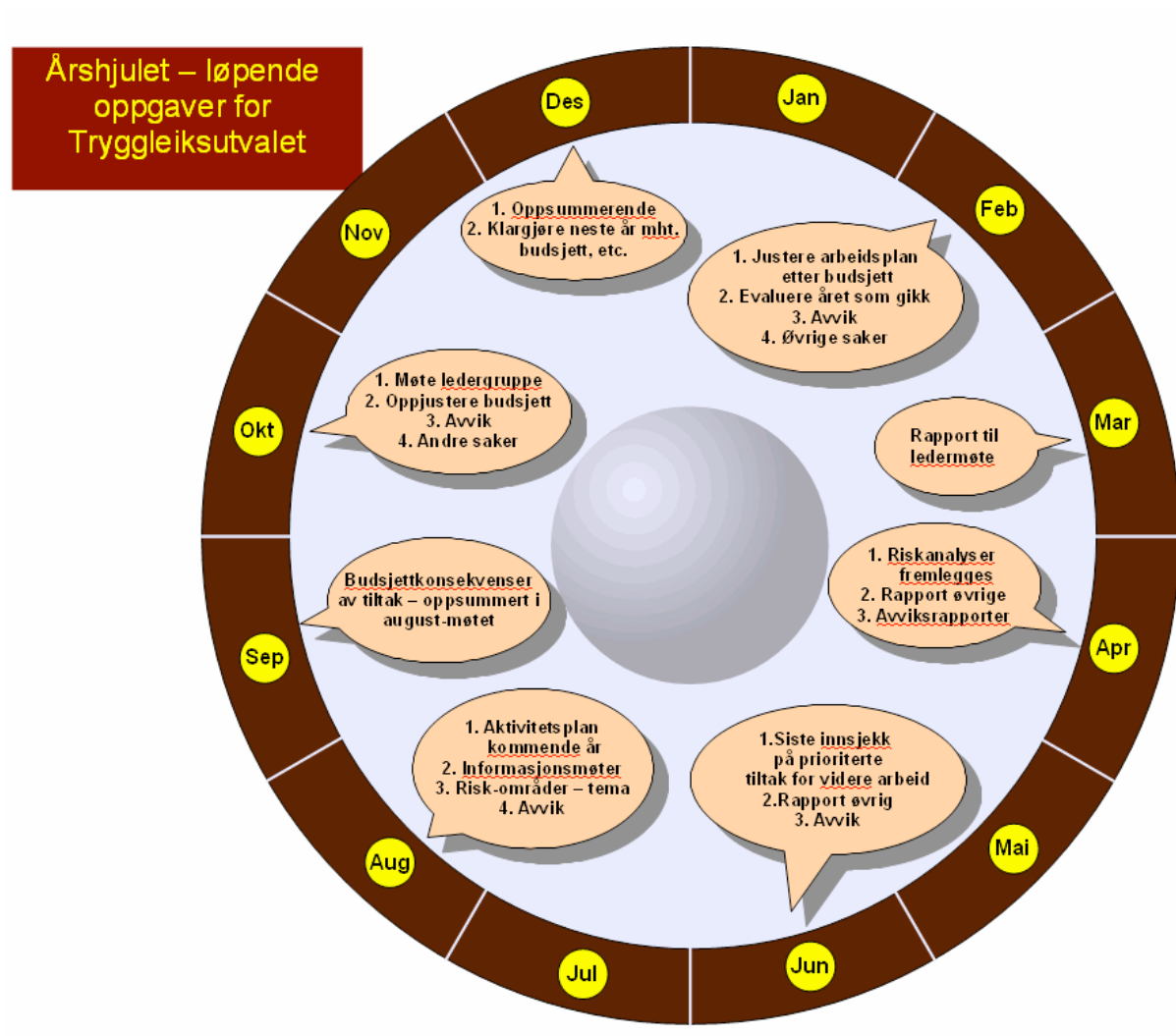
Tryggleiksutvalet skal i samarbeid med leiinga utarbeide ein plan for årleg kontroll for å stadfeste om arbeidet med verksemda sine informasjonssystem på kvar kontrollstad er i samsvar med administrative og tekniske rutinar.

- tryggleikskoordinator på avdelingane utfører kontrollane
- kontrollplanen skal vere godkjent av leiinga innan 1. februar
- kontrollen skal vere gjennomført innan 1. november
- kontrollrapporten skal vere eit grunnlag for leiinga sin gjennomgang (innan utgangen av året)

Kontrollane skal vere ein gjennomgang av :

- informasjonstryggleikshandboka for å sjekke at den er samsvar med behov og realitetar
- sikringsmåla
- sikringsstrategien
- organiseringa av tryggleiksarbeidet
- eigenkontrollar eller kontrollar utført av offentleg organ
- risikoanalysene som er utført
- avviksregistreringar (sjekk om dei oppdager systematiske avvik)
- endringar i offentlege krav (lovverk)
- ev. endringar i bruk av personopplysningar i etablerte informasjonssystem
- nye informasjonssystem
- dokumenterte behov for, eller planlagt innføring av nye informasjonssystem

Gjennomgangen skal dokumenterast ved å bruke skjemaet i kapittel 10.6 som mal.  
Skjemaet og underlag for gjennomgangen, skal arkiverast.



---

## 10. Vedlegg

### 10.1. Rammeverk for risikoanalyse

Analysen byggjer på dokumentet ”Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven”.

[http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering\\_TV-505\\_02.pdf](http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-505_02.pdf)

Denne rettleiinga skildrar ein metode for å oppfylle kravet Datatilsynet set til gjennomføring av risikoanalysar. Formålet med risikoanalysar er å finne ut om risikoen som blir funne er akseptabel. Er den ikkje det, må det treffast tiltak slik at den blir det.

I dette eksemplet har vi sett opp risikoanalyse for bruk av internettløysingar som e-post og webtilgang frå sikker sone i ei helseverksemd. Det er prøvd å lage eit rammeverk som tar utgangspunkt i dei viktigaste truslane, skildrar konsekvensar og moglege årsaker og lister opp nokre risikoreduserande tiltak. Denne analysen vurderer risikobildet knytt til integrering av e-post og web-system i eit arbeidsmiljø med sensitive personopplysningar, altså ei ”ei-kontoløysing” der det ikkje er naudsynt med inn- og utlogging mellom bruk av interne og eksterne system. Vi har foreslått aktuelle tiltak som må vurderast. Når vi har kome fram til risikonivået vil vi for kvar hending kunne vurdere om risikoen er innafør akseptkriteria. Vi kan ikkje sjå kvar hending isolert frå dei andre, sidan det i einskilde høve kan vere naudsynt å akseptere ein høgare risiko for ei type hending (for eksempel utilsikta utlevering av personopplysningar) for å få risikoen for ei anna type hending (for eksempel manglande beslutningsunderlag på lite brukarvennleg løysing) ned på eit akseptabelt nivå. I slike tilfelle må desse vurderingane dokumenterast og grunnigvast.

Sannsyn	Konsekvens			
	Ufarleg	Litt farleg	Kristisk	Katastrofal
Svært truleg				
Truleg				
Lite truleg				
Lite sannsynlig				

#### Leiinga sitt ansvar:

Ei risikoanalyse er eit beslutningsverktøy. Iverksetjing og vurdering av resultatata frå risikoanalysen er leiinga sitt ansvar. Leiinga skal vurdere kor stor grad av risiko organisasjonen kan akseptere. I samband med den årlege gjennomgangen av sikringsmål, strategi og organisering vil resultatet av risikoanalyser vere ein viktig del av grunnlaget.

---

## Iverksettjing

Risikoanalyse er ikkje ein prosess som skjer berre ein gong. Endringar som har betydning for den totale informasjonstryggleiken vil gjere det naudsynt å gjere nye analyser, i det meste av alle tilhøve som blir rørt av endringane. Eksempler på endringar som krev ny risikoanalyse og godkjenning frå leiinga er:

- Endring i klassifisering av opplysningar
- Registrerte endringar i brukaradferd/bruksmønster (info frå driftsovervåking)
- Endringar i trusselbildet
- Organisasjonsendringar
- Endra oppkobling til sikker sone
- Endra oppkobling til eksterne datanett
- Ekstern overføring av nye typar opplysningar eller til nye partnarar

## Planlegging og oppstart

Formålet med risikoanalysen må skildrast eintydig. All naudsynt informasjon som finst på førehand og som er naudsynt i gjennomføringa, må skaffast (sikringsmål og –strategi, rammevilkår, lovpålagte krav, eksisterande akseptkriterier osv.).

Risikoanalysen bør gjennomførast av ei arbeidsgruppe. Denne arbeidsgruppa må vere samansett av personar som har god innsikt i analyseobjektet. Det er og viktig å ha med personar som har kjennskap til risikoanalyser som metode (ev erfaring frå tidlegare analyser). Ein kompetent person som ikkje sjølv deltar i analysen bør foreta kvalitetskontroll på det utførte arbeidet.

## Skildring av analyseobjektet

Skildringa må omfatte alle element som skal analyserast.

- avgrensing, slik at det går tydeleg fram kva risikoanalysen omfattar, og kva som ikkje er med
- administrative og tekniske rutinar
- beredskapsplanlegging og rutinar for reservekopiering
- personalsikring (kompetanseplanar, rutinar for autorisasjon, teieplikt)
- fysisk sikring (tilgangskontroll, områdesikring, bygningsmessig sikring, tilhøve for strøm, vatn, elektromagnetisk påverking)
- informasjonssystemets konfigurasjon
- informasjonstypar og dataoverføringar internt i verksemda, og mellom verksemda og eksterne datanett
- kommunikasjonskanalar og tilknytingspunkt
- operativsystem og programvare
- eksisterande tryggleikstiltak

Når risikoanalyse skal gjennomførast i samband med endringar, er det viktig å skildre desse så godt som mogleg. På denne måten vil den vidare analysen kunne finne ev manglar på eit tidlegast mogleg stadium.

## 10.2. Mal for Risikovurdering

### Brudd-koder:

**K** = Konfidensialitet      **I** = Integritet      **T** = Tilgjengelighet

### Vurderingsskala – individuell for hver ulik sak:

<b>Sannsynlighet (angitt som antall pr. år)</b>	<b>1</b> Unnsannsynlig (en gang hvert 5 år eller sjeldnere)	<b>2.</b> Mindre sannsynlig (en gang hvert år)	<b>3.</b> Mulig (en gang hver måned)	<b>4.</b> Sannsynlig (daglig eller oftere)
<b>Konsekvens</b>	<b>1. Ubetydelig</b> * stans i system under 10 min * ingen uautorisert innsyn i personopplysninger	<b>2. Moderat</b> * stans i system under 30 min * uautorisert innsyn i enkelte personopplysninger og lovbrudd	<b>3. Alvorlig</b> * Stans i system i 4 timer * uautorisert innsyn i enkelte personopplysninger, mulighet for endring og brudd på lov	<b>4. Kritisk</b> * stans i system i 8 timer eller mer * fullt uautorisert innsyn eller mulighet for endring i alle pers. oppl. og brudd på lov.

### Selve vurderingen: (utfylt med et lite eksempel)

Nr	Brud på	Årsak/Trussel	Uønsket hendelse	San - synl	Kons	R (S*K)	Mulige konsekvenser	Eksisterende tiltak/ forslag til nye tiltak	Ansvarlig tidsfrist
1	K, I	Lønsslippene sendes via epost. Tilgang til epost via web kan gi uvedkommende tilgang til å lese fagforeningstilknytning	Fagforeningsopplysninger blir lest av uvedkommende på lønsslipp som kommer på web-epost	4	2	8	Informasjon om fagforeningstilknytning kan bli misbrukt av uvedkommende.	Har unngått å sende lønnsdata til generelle adresser / Bør vurdere å kode fagforeningstilknytning på lønslippen	
2	K, I	Noen organisasjoner har VPN tilgang til forhandlingsmodulen	Fagforeningslister blir lest av uvedkommende pga. web-tilgang til lønnsystemet	3	2	6	Informasjon om fagforeningstilknytning kan bli misbrukt av uvedkommende.	VPN er sikrere enn direkte adgang/ Underlagt strenge rutiner for utskrifter etc.	

### 10.3. Mal for avviksrapportering

<b>Avviksrapport for Møre og Romsdal fylkeskommune</b>		Skal sendast til driftsansvarleg
Avviksnr:		
<b>Formål:</b> Rapporten skal sikre at alle brot og moglege brot på sikringsrutinane blir registrert og behandla på forsvarleg måte.		
Beskriv avviket:		
Vedlegg:		
Beskriv førebels tiltak:		
Vedlegg:		
Avviksmeldar/dato:	Kommentar:	
Analyse av årsak:		
Vedlegg:		
Beskriv korrigerande tiltak:		
Vedlegg:		
Tryggleiksansvarleg/dato:	Kommentar:	
Evaluert av/ dato:	Kommentar:	

---

## 10.4. Avtale mellom skole/institusjon og ekstern partner

Vedlagt følger ein mal for avtale mellom skole/institusjon og ekstern partner.

### Leverandør/partnar:

#### 1. Ansvar

Leverandøren er ansvarleg for tryggleiksbrøt av eige personale og / eller anna personale som opptrer etter oppdrag fra leverandør eller som leverandør gjev tilgang til fylket sine installasjonar / regiseter m.v. Leverandøren kan ikkje engasjere ein tredjepart (underleverandør) til å utføre arbeidsoppgåver som følgjer av denne avtalen, utan at oppdragsgivar har godkjent dette og leverandøren har inngått kontrakt med tredjepart som har tilsvarende tryggleiksreglar.

#### 2. Teieplikt

Leverandøren sitt personale skal underteikne teieplikt-erklæring. Dei som underteiknar teieplikta skal gjerast kjent med kva dette inneber. Leverandøren kan berre nytte dei personane til oppdraget som oppdragsgivar på førehand har godkjent og er informert om. Teieplikta gjeld også etter at avtalen er opphøyr, og etter at leverandøren sitt personell har slutta hos leverandøren.

#### 3. Tryggleiksløysing

Leverandøren skal til ein kvar tid ha ei organisatorisk og teknisk tryggleiksløysing som tilfredstillar Datatilsynet sine retningslinjer. Dette skal leverandøren kunne dokumentere for oppdragsgivar og Datatilsynet.

#### 4. Samarbeid

Leverandøren skal ved behov samarbeide med oppdragsgivar om dei tryggleiks-brøt som kan tilskrivast leverandøren. Som ledd i verksemda sin årlege eigenkontroll, bør det vere eit møte for å gå gjennom leverandøren sine organisatoriske og tekniske tryggleikstiltak.

### 5. OVERSIKT OVER PERSONELL HOS LEVERANDØREN SOM FÅR TILGANG TIL OMRÅDE OG UTSTYR

---

---

### 6. TEIEPLIKT-ERKLÆRING

Underskrift frå leverandør/partner og personell:

---

---

## 10.5. Rutine for tryggleikskopiering

<b>Komponent som skal kopierast</b>	<b>Dagkopi (SAN)</b> 1.intervallkopi 2.kopieringsmåte 3.medium	<b>Intervallkopi (fjernlagring)</b> 1.intervallkopi 2.kopieringsmåte 3.medium
Basisprogramvare til brannmurar, serverar og anna utstyr	1.Ved kvar ny versjon 2.Ein komplett kopi 3.Disk, CD-rom m.v.	1.Ved kvar ny versjon 2.Ein komplett kopi 3.Disk, CD-rom m.v.
Konfigureringar og innstillingar for brannmurar, serverar og anna utstyr	1.Ved kvar ny konfigurering 2.Ein endringskopi 3.Disk, tape m.v.	1.Ved kvar ny versjon 2.Ein komplett kopi 3.Tape m.v.
Sensitive personopplysningar	1.Rullerande kopi i 5 gen. 2.Disk/tape	1.Vekekopi 2.Ein komplett kopi 3.Tape m.v.
Personopplysningar	1.Rullerande kopi i 5 gen. 2.Disk/tape	1.Vekekopi 2.Ein komplett kopi 3.Tape m.v.
Andre data	ved behov	ved behov

---

## 10.6. Forslag til møteinnkalling for gjennomgang av informasjonstryggleiken med leiing

Under er det laga ein mal for møteinnkalling for ein gjennomgang med leiinga. I tillegg til leiinga skal IT-koordinatoren og tryggleiksleiaren delta i gjennomgangen.

Rapport frå leiinga sin gjennomgang 2006	Verksemd:	Skrive av:	Dato: xx.12.0 6	Arkivref:
Deltakarar:			Distribusjon:	
Saknr	Sak	Aksjon	Ansv. frist	
1/06	Rapport frå utførte internkontrollar og ev. kontrollar utført av offentleg myndigheit			
2/06	Behandling av registrerte avvik			
3/06	Resultat frå risikovurderingar (for eksempel endringar i truslar)			
	Vurdering av ev. endringar i offentlege tryggleikskrav			
	Informasjon om den faktiske bruk av interne informasjonssystem			
	Mål og strategiar for informasjonstryggleik			
	Oversikt personopplysningar som blir behandla elektronisk			