Rauma kommune

Styringssystem for personvern og informasjonssikkerheit i Rauma kommune 2021 - 2024

Vedtatt av kommunestyret 30.09.2021, sak PS-72/21

INNHOLD

1. Innleiing

1.1 Formål med styringsdokumentet

Dette dokumentet er det overordna styringsdokumentet for informasjonssikkerheit i Rauma kommune. Dokumentet inneheld målsetjingar og strategiar som er rekna som nødvendige for å oppnå tilfredsstillande informasjonssikkerheit i kommunen (også kalla organisasjonen), og den gjennomgår lovgrunnlaget og ansvarsfordelinga mellom leiinga, IKT og andre tilsette.

I dokumentet viser vi til personopplysningslova med personvernforordninga, også kalla GDPR-forordninga eller personvernforordninga.

1.2 Kommunen sine trusselaktørar

Kommunen står ovanfor ulike truslar som kan påverke styringssystemet og forvaltning av dette. Kvart år presenterer Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Etterretningstjenesten kva truslar samfunnet står ovanfor. Kommunen må følgje anbefalingane som kjem frå desse aktørane for å redusere risikoen for angrep på vår infrastruktur og informasjonssystem.

Kort fortalt om truslar:

1.2.1 Eksterne truslar

Truslar i det digitale rommet er noko kommunen står ovanfor kvar dag. Vi ser tilfelle av at både kommunar og statlege aktørar vert «hacka,» og informasjonssystema vert slått ut. Måten trusselaktørane får tilgang til informasjonssystema våre på, er mange og ulike. Det kan vere gjennom ei lenke i ei e-postmelding som tilsette trykker på, eller via ein svakheit i vår infrastruktur.

Korleis skal kommunen drive sine tenester dersom den digitale infrastrukturen vert slått ut? Er kommunane og einingane budd på å drifte tenesta i kortare eller lengre tid utan tilgang til fagsystem og telefonitenester? Kompetanse i organisasjonen, jf. kap. 11, gode internkontrollprosedyrar i kommunen, hos einingane og IKT for å sikre god og sikker drift, jf. kap. 7, 8, 9 og 10 i styringsdokumentet.

1.2.2 Interne truslar

Når det gjeld interne «truslar», så kan manglande kompetanse blant tilsette vere ein risiko. At kommunen si leiing og tilsette ikkje har god nok kompetanse på korleis ta vare på og sikre kommunal informasjon, kan føre til at eksterne trusselaktørar lettare får tilgang til informasjonssystema våre. I verste fall lamme tenestene våre. Fokus på god sikkerheitskultur i heile organisasjonen er eit kontinuerleg arbeid, jf. også kap. 11 om kunnskap, kompetanse og kultur.

1.2.3 Oversikt over verdiar

At kommunen har oversikt over kva verdiar som må beskyttast og har gode kontrollrutinar (system for internkontroll) og gjennomfører leiinga sin gjennomgang, vil avdekke svakheiter og vi kan setje inn tiltak for å redusere risikoen.

Nøkkelordet for å redusere risikoen er «kontinuerleg arbeid med informasjonssikkerheit og personvern», jf. også kap. 4 i styringsdokumentet om kva informasjonsverdiar kommunen skal beskytte.

1.3 Kven gjeld styringssystemet for?

Styringssystemet gjeld for alle system, applikasjonar, IKT-utstyr, forretningsprosessar, informasjon/data, administrative funksjonar, nettverk, tilsette, innleigde, samt bygningar og utstyr som blir brukt for å drive kommunen.

1.4 Å forvalte informasjon

Informasjon og informasjonssystem representerer store verdiar, og bør av den grunn behandlast som strategiske ressursar på line med for eksempel bygningar, produksjonsutstyr og kapital, og bør sikrast deretter. Informasjonen må vernast slik at truverdigheita vert oppretthalden og kvaliteten og nøyaktigheita er slik brukaren forventar. Det er eigaren av informasjonen som må fastsetje kva verdi eller sensitivitet informasjonen har, og følgjeleg sørgje for at sikringa er tilstrekkeleg. Det er behandlingsansvarleg[1] i Rauma kommune som er eigar av informasjonen.

1.4.1 Tenesteleg behov

For å sikre visse typar informasjon, er det viktig at informasjon er gradert og at graderinga er formell og riktig. Det er viktig at tilsette får forståing for kvifor det er nødvendig å gje den einskilde medarbeidaren tilgang til ulike typar personopplysningar og IT-system, basert på behova den tilsette har for å utføre oppgåvene sine.

1.4.2 Openheit

Det er ei forventning om at kommunen skal vere open mot innbyggjarane, media og omverda. Alle som ønskjer å vite kva som skjer og som vil følgje eller påverke avgjerder, skal kunne gjere det.

Innbyggjarane har ei særleg forventning om at personopplysningane vert behandla konfidensielt og vert oppbevart på ein sikker måte. Kommunen si leiing og dei tilsette har ei forventning om at kommunen sine data blir behandla i samsvar med kommunen sitt styringssystem for personvern og informasjonssikkerheit.

Kva innbyggjarane har rett til å få informasjon om, er mellom anna regulert i offentleglova. I kommunen sitt arbeid med informasjonssikkerheit, skal også openheit takast omsyn til så lagt det let seg gjere, jf. personvernforordninga artikkel 5.(1).(a).

1.4.3 Fysisk sikring og tilgangskontroll

Fysiske og driftstekniske sikringstiltak er viktig for å sørgje for heilskapleg informasjonssikkerheit for organisasjonen. Dette gjeld om organisasjonen driftar systema i eige hus, har utkontraktert systema eller bruker ulike formar for skyløysingar.

Fysiske sikringstiltak omfattar mellom anna tilgangsstyrt inngang til lokale, sikre serverrom mot brann- og vasskadar, verksemdkritiske maskiner og utstyr er låste inn i eigne skap/rom, med meir.

Tilgangskontroll er viktig for å oppdage eller forseinke ein inntrengar, samt å redusere skade på verdiar, for eksempel tilgangskontroll til lokalar og tilgangskontroll til it-system.

1.4.4 Dokumentforvaltning og arkivering

Nedanfor er det gitt ei samla oversikt over nødvendig dokumentasjon, og reglar for lagring av

[1] Kommunen/kommunedirektøren er behandlingsansvarleg. Leiar vert definert som dagleg behandlingsansvarleg i eiga eining.

historiske dokument.

Dokumentasjon om tiltak knytt til informasjonssikkerheit skal sikrast på tilsvarande måte som helse- og personopplysingar når kjennskap til tiltaka for uvedkomande vil innebere ein risiko.

Dokument i samband med arbeidet med informasjonssikkerheit skal oppbevarast slik:

Emne	**Oppbevaring/arkivering**
Internkontroll	Saks- og arkivsystemet
Eigenkontroll	Saks- og arkivsystemet
Leiinga sin gjennomgang	Saks- og arkivsystemet
Risikovurderingar- og analyser	Saks- og arkivsystemet
Prosedyrar	Internkontrollsystemet
Behandlingsprotokollar	Sureway/Personvernappen

1.5 Eigaransvar

For å kunne forvalte personvernforordninga på ein god og sikker måte, må leiarar og tilsette ha oversikt over kommunen sine plikter (vedlegg 1. 3) og den registrerte sine rettar (vedl. 1. 4). I tillegg skal behandlingsansvarleg sørge for at leiarar og tilsette har kompetanse på området (kap. 11) og gjennomfører dei oppgåvene som ligg til den enkelte (kap. 5).

1.6 Kommunen sitt avvikssystem

IK/HMS er kommunen sitt system for avviksbehandling.

2. Krav til internkontroll og styringssystemet

2.1 Krav til internkontroll

Personopplysningslova stiller krav til internkontroll i form av planlagde og systematiske tiltak som er nødvendige for å oppfylle krava i eller i medhald av personopplysningslova, medrekna å sikre kvaliteten av personopplysningane.

Føresetnaden for å gjennomføre ein internkontroll, er at det er ein felles forståing i organisasjonen av kva risiko er og korleis risiko av ulik grad skal handterast.

Eigenkontrollen skal sikre at vedteke sikkerheits- mål og strategi og organisering vert etterlevd i heile kommunen. Resultatet av eigenkontrollen dannar grunnlag for eventuelle endringar i sikkerheit, strategi og organisering, og inngår i underlaget for leiinga sin årlege gjennomgang av informasjonssystemet og informasjonssikkerheita.

Internkontrollsystemet gjeld for heile organisasjonen og implementering av internkontrollsystemet krev at:

- Alle som er involvert i behandling av personopplysningar[2], skal gjere seg kjent med prosedyrar og retningsliner for personvern og informasjonssikkerheit. Prosedyrane er lagra i internkontrollsystemet og alle er merka med «GDPR».
- Alle tilsette skal få relevant opplæring og ha relevant kunnskap ut frå si rolle i organisasjonen.
- Alle tilsette skal medverke til forbetringar gjennom forbetringsforslag og avviksrapportering.
- All dokumentasjon (prosedyrar og planverk) skal vere oppdatert og gjenstand for revisjon.
- Leiinga skal gjennomføre ein systemrevisjon og leiinga sin årlege gjennomgang.

Ansvaret for gjennomføring av internkontrollen er fordelt slik:

- Behandlingsansvarleg har ansvar for at internkontrollsystemet er i bruk og implementert i organisasjonen
- Sikkerheitsleiar har det faglege ansvaret på vegner av rådmannen for at systemet er oppdatert i samsvar med lovkrav og interne krav.
- Leiar har ansvar for at tilsette har fått opplæring i bruk av internkontrollsystemet og blir oppfordra til å bruke systemet.
- Leiar har ansvar for å utarbeide nødvendig dokumentasjon, behandle avvik/hendingar og gjennomføre risikovurderingar. Samt drive førebyggjande- og forbetringsarbeid
- Tilsett har ansvar for å bruke systemet for å gjere seg kjend med organisasjonen sine dokument og melde inn avvik og forslag om forbetringar.

Kommunen har eige skjema for gjennomgang av internkontroll.

Kommunens årshjul for personvern og informasjonssikkerheit skal seie noko om når dei ulike aktivitetane skal gjennomførast.

[2] Behandling av personopplysningar; Når ein borgar t.d. søkjer om ein barnehageplass, behandlar kommunen personopplysningar om søkar og barnet som skal i barnehagen (namn, personnummer, adresse med meir).

2.2 Kommunen sitt avvikssystem

2.2.1 Plikt til å melde avvik[3]

Alle tilsette har ein plikt til å melde avvik for brot på personvern og informasjonssikkerheit så snart som muleg på eige skjema (krav til innhald frå Datatilsynet). Avviket vert meldt til næraste leiar med kopi til sikkerheitsansvarleg.

Eit brot på personopplysningssikkerheita kan kategoriserast i (jf. Vedlegg 1-5):

- Brot på konfidensialitet.
- Brot på integritet.
- Brot på tilgjengelegheit.

Eit brot kan omfatte ein, eller ein kombinasjon av desse tre. Det avheng av omstenda. Det er etablert eigne prosedyrar for melding av avvik.

2.2.2 Melde avvik til Datatilsynet

Den behandlingsansvarlege har plikt til å melde avvik til Datatilsynet så snart som muleg etter avviket er oppdaga og innan 72 timar. Den behandlingsansvarlege skal, saman med personvernombodet, vurdere om avviket skal meldast vidare til Datatilsynet.

2.2.3 Mottatt melding om avvik meldt av andre

Den behandlingsansvarlege skal behandle avvik meldt av andre (databehandlar, innbyggjar, brukar m.fl.) på lik line som avvik meldt av eigne tilsette. Kommunen har plikt til å varsle Datatilsynet innan 72 timar etter avviket er oppdaga. Kommunen legg seg på same praksis dersom Datatilsynet bør varslast om avviket meldt av andre.

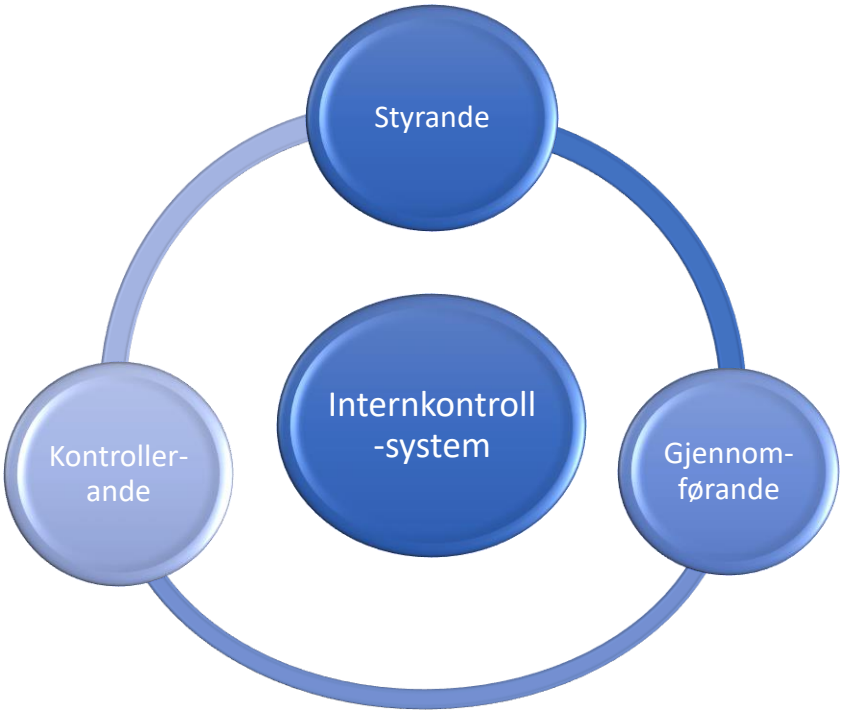
2.3 Rauma kommune sitt styringssystem

Det er ulike lovverk som seier noko om kommunen si plikt å ha eit styringssystem:

- Personvernforordninga: Artikkel 32 «Sikkerhet ved behandlingen»
- e-forvaltningsforskriften kapittel 3: Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet».
- Normen: Faktaark 2 «Styringssystem for informasjonssikkerhet» og faktaark 3 «Dokumenter i styringssystemet»
- Digitaliseringsrundskrivet refererer til eForvaltningsforskriften

[3] Avvik: Hending eller ein situasjon som bryt med gjeldande lovverk, regelverk eller kommunen sine prosedyrar.

Styringssystemet i Rauma kommune er bygd opp slik:



Vedlegg nr. 2 inneheld ein oversikt over prosedyrane knytt til styringssystemet.

2.3.1 Styrande del

I den styrande delen er det forklart kven og kva styringssystemet skal gjelde for i kommunen. Alle funksjonane og prosessane som er lista opp nedanfor er regulert i eigne prosedyrar som ligg i IK/HMS.

- Definere sikkerheitsmål og sikkerheitsstrategi.
- Plan for å nå sikkerheitsmåla.
- Definere roller, ansvar og myndigheit i forhold til informasjonssikkerheit i kommunen.
- Plan for opplæring og bevisstgjering av tilsette.
- Fastsette akseptabelt nivå av risiko og når risikovurderingar skal gjennomførast
- Ha oversikt over kva for opplysningar kommunen behandlar og oversikt over kritiske system (kommunal beredskapsplikt) og eventuelt kva klassifisering systema har.
- Ha ein sikkerheitsinstruks/akseptabel bruk regel for alle tilsette og innleigde i kommunen.
- Kven samhandlar kommunen med og kven gjer kva.

Leiinga i kommunen skal vise sitt engasjement til sikkerheit ved å:

- Sjå til at kommunen har ein sikkerheitsstrategi med sikkerheitsmål som er i tråd med kommunens overordna mål og strategiar.
- Sørge for implementering av styringssystemet i kommunens eksisterande rutinar og prosessar.
- Allokere ressursar (personar og pengar) til implementering av styringssystemet.
- Sørge for at dei som har roller knytt til informasjonssikkerheit og personvern har nok kompetanse og støtte frå leiinga.
- Være pådrivar og førebilde for dei tilsette med tanke på personvern og informasjonssikkerheit.

2.3.2 Kontrollerande del

I den kontrollerande delen må kommunen sørge for at dei har eit system for avviksrapportering og sikkerheitsrevisjonar. Alle funksjonane og prosessane som er lista opp nedanfor er regulert i eigne prosedyrar som ligg i IK/HMS.

For at kommunen skal kunne vite at styringssystemet fungerer, må kommunen:

- Ha eit system for avviksmeldingar og kontinuerleg forbetring (oppfølging av avvik).
- Sjå til at leiarar som tek i mot avvik følgjer opp desse og har rutinar for varsling av dei registrerte og tilsynet.
- Ha ein plan for kva revisjonar som skal gjennomførast. Desse skal ligge i årshjulet.
- Sørge for at alvorlege avvik og resultat frå revisjonar vert rapportert under Leiinga si gjennomgang. Leiinga sin gjennomgang er omtala i kapittel 10 i styringsdokumentet.

2.3.3 Gjennomførande del

Den gjennomførande delen inneheld reglar og krav til personvern og informasjonssikkerheit som tilsette i kommunen skal følgje. Alle funksjonane og prosessane som er lista opp nedanfor er regulert i eigne prosedyrar som ligg i internkontrollsystemet.

- Teknisk dokumentasjon av system med tilhøyrande konfigurasjonskart, sikkerheitsarkitektur og iverksette tiltak.
- Oversikt over databehandlarar og leverandørar, samt behandlingsoversikt og oversikt over kritiske system.
- Årshjul for informasjonssikkerheit:
    - Plan for risikovurderingar og oppfølging av tiltaksplanar etter risikovurderingar.
    - Opplæring og tiltak for bevisstgjering.
    - Revisjonar.
    - Oppfølging av sikkerheitsmål.
- Kommunen bør også vurdere om ein skal ha prosedyre for:
    - Gjennomføring og oppfølging av risikovurderingar.
    - Klassifisering av verdiar.
    - Internkontroll.
    - Endringshandtering.
    - Bruk av databehandlarar.
    - Andre prosedyrar basert på valde kontrollar/tiltak etter heiskapeleg risikovurdering.

I gjennomførande del har vi også prosedyrar for administrative og daglege aktivitetar slik:
I den administrative delen er det fokus på mellom anna dei registrerte sine rettar etter GDPR-forordninga, og kommunens behandling av personopplysningar. Alle funksjonane og prosessane som er lista opp nedanfor er regulert i eigne prosedyrar som ligg i IK/HMS.

- Innsamling av personopplysningar.
- Innsyn, retting og sletting av personopplysningar.
- Føring av behandlingsprotokoll.
- Risikovurdering.
- Melde avvik og varsling

Den daglege delen inneheld ulike prosedyre på dei tilsette sine pliktar til å ivareta personvern og informasjonssikkerheit.

2.4 Revisjon og oppfølging av styringsdokumentet

Styringssystemet krev at det blir gjennomført revisjonar av både styringssystemet i seg sjølv, rutinar og prosedyrar som støttar styringssystemet. Årshjulet skal vise når dette er planlagt gjennomførd.

Kommunen har ein eigen prosedyre for revisjon av styringssystemet, samt revisjon av rutinar og prosedyrar som støttar styringssystemet.

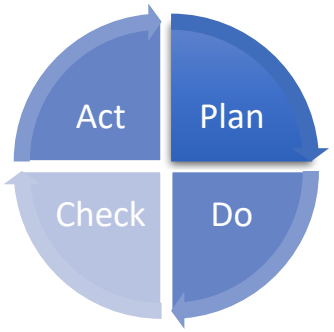
Styringsdokumentet skal opp til politisk behandling ein gong kvar kommunestyreperiode. Styringssystemet er gjeldande frå vedtaksdato.

2.4.1 Å oppnå kontinuerleg forbetring av styring av personvern og informasjonssikkerheit

Kommunen vil følgje prinsippa for PDCA-tilnærming (Plan, Do, Check, Act) i forbetringsarbeidet med oppdatering og forbetring av arbeidet med personvern og informasjonssikkerheit:

- Plan: Definere problemet ved å t.d. gjennomføre risikoanalysar og identifiser potensielle kontrollar for å redusere kommunen si risikoeksponering.
- Do = Implementer kontrollar.
- Check = Gjennomfør internkontrolltiltak, som internrevisjon, for å verifisere om kontrollane fungerer. Kommunen skal gjennomføre «leiingas gjennomgang» og identifisere kva for kontroll som ikkje fungerer og foreslå tiltak for å handtere manglar/kontrollar som ikkje fungerer.
- Act = Implementere endringsforslag/nye kontrollar.

PDCA er ein del av leiinga sin gjennomgang.



2.4.2 Oppdateringar utover kommunestyreperioden

Det er eit krav at sikkerheitsmåla og sikkerheitsstrategien vert oppdatert årleg i samband med leiinga si gjennomgang. Dette på grunn av at IKT-området og risikobildet er i stadig endring og måla må reviderast i takt med desse endringane. Dersom det vert gjort større endringar for sikkerheits-måla og strategien, vert det lagt fram ei sak om det til kommunestyret. Andre endringar som t.d. nasjonale føringar og resultat av sentrale og lokale trusselvurderingar, vert lagt fram som ei orienteringssak til kommunestyret om det er av større betydning.

2.4.3 Ansvar for oppfølging av styringsdokumentet

I samsvar med ansvarsprinsippet i sikkerheitsorganisasjonen, har behandlingsansvarleg ansvar for styringssystemet vert etterlevd og leiar har ansvaret for å følgje opp planverket med tilhøyrande prosedyrar på sitt ansvarsområde. Sjå meir om ansvar i styringsdokumentet kap. 4 og 5.

3. Kva verdiar skal kommunen beskytte?

Rauma kommune skal ha oversikt over kva verdiar kommunen må beskytte, samt kva tiltak som må setjast i verk for å kunne drifte eininga dersom verdien ikkje er tilgjengeleg.

3.1 Kartlegging av informasjonsverdiar

Når det gjeld verdiar knytt til personvern og informasjonssikkerheit, så bør kommunen beskytte følgjande sentrale verdiar:

- Informasjon.
- Personopplysningar.
- Sensitive personopplysningar.
- Informasjonssystemet.
- Tilgangsstyring til bygningar og eigedomar for å sikre ulike system, ulike type hardware som nettbrett, servere, PC, arkivmateriale og liknande.

Kommunen skal til ein kvar tid ha oversikt over eigne kritiske verdikjeder og når brot i desse verdikjedene fører til krisesituasjonar som gjer det nødvendig å iverksette beredskapsplanar.

3.2 Tiltak og beredskapsplan

Når kartlegginga er gjennomført/oppdatert og tiltaka for å redusere sårbarheita er identifisert, må kommunen setje i verk tiltak for å kunne drifte tenestene i kritiske situasjonar. Korleis tenesta skal driftast i ein krisesituasjon/sårbar situasjon, må stå forklart i einings si beredskapsplan. Les meir om beredskap i styringsdokumentet kap. 10.

3.3 Ansvarleg for kartlegging av verdiane

Behandlingsansvarleg er ansvarleg for kartlegging av verdiane (informasjonsflyten) i eigen organisasjon for å avdekke kritiske konsekvensar/sårbarheiter for eventuelt tap eller reduksjon av denne verdien. I tillegg må leiar kartlegge kva verdikjedar dei er ein del av og sårbarheiter i desse kjeda.

4. Sikkerheitsmål og sikkerheitsstrategi

4.1 Sikkerheitsmål

Sikkerheitsmåla skal støtte og sikre at alle tilsett veit korleis behandling av personopplysingar skal skje i det daglege.

Sikkerheitsmåla skal sikre at personopplysingar blir handterte i samsvar med lovkrav og interne avgjerder.

Sikkerheitsmåla gjeld for alle tilsette i organisasjonen og er følgande:

1. Vi skal sikre at informasjon blir behandla i tråd med krava i relevante lover og forskrifter.
2. Vi har sikkerheita forankra hos kommunedirektøren og leiinga.
3. Vi skal ta i vare sikkerheita som ein integrert del av heile kommunen sin organisasjon.
4. Den fysiske sikkerheita ved kommunen skal hindre at uautoriserte får tilgang til lokalar der sensitive personopplysingar og annan informasjon som ikkje skal offentleggjerast, blir lagra og behandla.
5. Vi skal sikre at uautoriserte ikkje får elektronisk tilgang til kommunens informasjon som inneheld beskytta informasjon og/eller sensitiv informasjon.
6. Vi skal ha tilgang til system og informasjon etter tenesteleg behov.
7. Vi skal sikre at informasjonsbehandlinga er korrekt i forhold til formål og heimel til behandlinga, og at informasjon ikkje kan forandrast utan lovleg tilgang.
8. Vi skal sikre at tilgang til system, tenester og informasjon til rett tid for dei personane som er autorisert.
9. Vi skal sikre at det er mogeleg å spore uønskte hendingar. Prosedyrar for å handtere uønskte hendingar skal vere oppdaterte og kjende.
10. Vi skal korrigere og lære av hendingar som kan føre til brot eller mistanke om brot på personvernet.
11. Vi skal sikre at personar eller system hos kommunen - medviten eller umedviten – ikkje skal vere årsak til sikkerheitsmessige uønskte hendingar som truar informasjonsvernet til eigen organisasjon, andre si verksemd eller til privatpersonar.
12. Vi skal sikre at medarbeidarar som nyttar kommunen sine informasjonssystem har tilstrekkeleg kompetanse for å vareta organisasjonen sitt sikkerheits-behov/krav.
13. Vi skal sikre at kommunen til ein kvar tid har sikkerheit på sine IKT system som gjev
    - **Rett informasjon:**
      Personinformasjon og anna informasjon som ligg i våre system skal til ein kvar tid vere oppdatert
    - **Til rett tid:**
      Systema skal være tilgjengeleg.
    - **Til rett person:**
      Tilsette skal ha tilgang til dei opplysningane som er nødvendig

Vi skal sikre at informasjonen

- Ikkje vert kjent for uvedkommande = KONFIDENSIALITET
- Ikkje vert endra utilsikta eller av uvedkommande = INTEGRITET
- Er tilgjengeleg ved behov = TILGJENGELEGHEIT

4.2 Sikkerheitsstrategi

Sikkerheitsstrategien skal konkretisere korleis ein arbeider for å vareta sikkerheitsmåla for organisasjonen.

4.2.1 Aktivitetar

Akseptabel nivå av risiko

- For alle system skal det fastsettast nivå for akseptabel risiko for systemets tilgjengelegheit, konfidensialitet, integritet og kvalitet.

Risikovurdering

- Ei risikovurdering er eit verktøy for å identifisere uønskte hendingar og risikoen for at desse skal hende. Risiko har to dimensjonar: skadeverking (konsekvens av eit sikkerheitsbrot hender) og sårbarheit (sannsynlegheit for at eit sikkerheitsbrot hender). Risikovurderinga må sjåast i samanheng med etablert akseptkriterium for risiko, og den behandlingsansvarlege skal setje i verk nødvendige tiltak for å oppnå tilfredsstillande informasjonssikkerheit.
- Sjå meir om ROS i kapittel 6 i styringsdokumentet.

Kontraktar

- Alle formalitetar mellom kommunen og leverandørar skal vere formulerte i formelle kontraktar (SLA - Service Level Agreement) og skal inkludere relevante sikkerheitskrav.
- Register/datasystem som leverandørar driftar på vegner av kommunen skal sikrast gjennom ein databehandlaravtale.
- Forordninga krev at det vert etablert ein databehandlaravtale i alle tilfelle kor forordninga krev at «en behandling skal utføres på vegne av en behandlingsansvarlig», jf. art. 28. (1). Det kan være tilfelle der ein tredjepart behandlar personopplysningar på vegne av kommunen utan at tredjeparten driftar eit datasystem for kommunen.

Eigenkontroll

- Eigenkontroll/måling av sikkerheitsnivå ved kommunen skal utførast regelmessig i samsvar med prosedyrar.
- Sjå meir om eigenkontroll i styringsdokumentet kap. 8.

System

- Einingsleiar er ansvarleg/eigar av dei fagsystema/behandlingar som er spesifikke for eininga si.
- Behandlingsansvarleg (kommunedirektør) utpeiker systemansvarleg og eigar på dei systema som blir brukte av fleire einingar.
- Dagleg vedlikehald, tryggleik og drift blir varetatt av organisasjonen sin IT eining, dersom løysinga er lokal.
- Administrasjon av endringar/rettar i systemet blir varetatt av einina.

Tilgang til informasjonssystem/behandlingar

- Leiar er ansvarleg for å klarleggje og autorisere den einskilde tilsette sitt behov for tilgang, og skal formidle dette til IT-ansvarleg/systemadministrator.
- Einingsleiar er ansvarleg for å melde til IT-/systemansvarleg at personell sluttar, slik at tilgangsrettar blir fjerna.
- Kommunen skal ha ei oversikt over dei tilgangsrettane som er gitt.
- Kommunen skal ha ein enkel oversikt over kva personsensitive opplysningar kommunen behandlar og kva fagsystem som behandlar desse. Einingsleiar er ansvarleg for at det er oppretta protokollar for behandling av personopplysningar i si eining.

- Kommunen har også prosedyrar som hindrar uautoriert tilgang til person- og helseopplysningar og uautorisert endring av slike opplysningar.
- Oversikt over kva personopplysningar kommunen behandlar, er beskrive i behandlingsprotkollane.

Kommunikasjonsløysingar

- Kommunikasjonsløysingar som blir nytta ved overføring av personinformasjon og sensitiv informasjon skal sikrast i samsvar med godkjente løysingar.

Generell teieplikt

- Alle som får tilgang til kommunen sine personopplysingar og informasjonssystem skal underskrive erklæring om teieplikt.
    - Teieplikt for tilsette og politikarar.
    - Teieplikt for eksterne aktørar.

Sikkerheitsinstruks/databrukaravtale

- Tilsette med tilgang til informasjonssystema skal få ein gjennomgang av retningslinjer for informasjonssikkerheit.
- Tilsette skal signere ein databrukaravtale før dei får tilgang til informasjonssystema.

Opplæring

- Ved innføring av nye system/oppdateringar/nye tilsetjingar er leiar ansvarleg for at opplæring blir gitt.
- Opplæringa skal sikre at alle tilsette er kjende med det ansvaret det er å behandle personopplysingar, sensitive personopplysingar, elektronisk, munnleg og fysisk (papir).
- Meir om opplæring, sjå kap. 11 i styringsdokumentet.

Soneinndeling og tilgangskontroll

- Tilgang til lokalar der det blir behandla/oppbevara person-, sensitive personopplysingar skal sikrast mot uvedkomande.
- Arkiv, serverrom og rom med anna sentralt IT-utstyr skal sikrast slik at det er mogeleg å avgrense tilgangen til området.
- Ytterdører skal vere låste etter arbeidstida sin slutt.

Dokumentsikkerheit

- Alle dokument med personopplysingar skal bli oppbevart, sendt og makulert på ein trygg måte.
- Konfigurasjon og konfigurasjonskontroll: Tilpassing og innstilling av eit datasystem eller programvare.
- Leiar har ansvaret for å utarbeide og vedlikehalde oversikt over utstyr, programvare og systemkonfigurasjon.

Endringskontroll

- Ved endringar/innføring av informasjonssystem skal det vurderast kva konsekvensar dette kan få for tryggleiken.
- Endringar som kan ha konsekvensar for informasjonssikkerheita, skal drøftast og godkjennast av behandlingsansvarleg/sikkerheitsleiar/arkivleiar/personvernombod, eller eit sikkerheitsutval.
- For endringar av fellessystem som kan ha konsekvens for sikkerheita, skal det utarbeidast ei risikovurdering inkludert forslag til tiltak.

Beredskap

- Einingane skal ha plan for å sikre normaldrift.
- Meir om beredskap, sjå kap. 10 i styringsdokumentet.

Tiltak for å hindre uhell/kriser

- Brann:
    - Brannsløkkingsutstyr skal vere tilgjengeleg.
    - Brann, straumbrot eller andre uhell skal ikkje kunne slette eller øydeleggje informasjon.
- Vatn:
    - Sikring mot vasslekkasje i relevante rom.

Avviksbehandling

- Hendingar for personvern skal alltid rapporterast til nærmaste leiar via organisasjonen sitt internkontrollsystem
- Behandling av hendingar/avvik skal følgje organisasjonen sin prosedyre for avvikshandtering.
- Meir om avvik, sjå kap. 2 i styringsdokumentet.

Systemteknisk sikkerheit

- It-avdeling eller driftspartnar skal ha ein oppdatert plan for systemteknisk sikkerheit.

Krav til dokumentasjon

- Det skal føreligge ei oversikt over behandling av personopplysingar (protokollar)
- Prosedyrane skal vere oppdaterte
- Risikoanalysar skal vere oppdaterte
- Referat frå leiinga sin gjennomgang skal arkiverast
- Skisse som viser samankopling av infrastruktur
- Driftsdokumentasjon for It-systema (ved lokal drift)

Infrastruktur

- Mekanismar i nettverkskomponentar, operativsystem og anna programvare skal brukast for at tilsette berre har tilgang til relevant informasjon.
- Automatisk passordbeskytta skjermsparer skal nyttast.
- Systema skal regelmessig oppdaterast med relevante sikkerheitsløysingar
- Servar og klientar skal vere hindra mot innbrot og nedetid.
- PC som ikkje er kommunal eigedom, skal ikkje koplast til kommunen sitt nettverk.
- All PC'ar knytt til kommunen sitt nettverk skal vere innkjøpt, forvalta og konfigurert av IT-ansvarleg.
- Det skal ikkje lagrast sensitive opplysingar på berbar medium som kan fjernast frå kommunen sine lokale.
- Informasjonssystem skal vere konfigurert til å logge uautorisert tilgang eller forsøk på uautorisert tilgang.
- Tilgang relatert til brukarar skal vere sporbart til brukarnamn/-identifikasjon
- Programvare- og maskinvareplattformer nytta i kommunen sitt informasjonssystem skal vere standardiserte.
- Det er ikkje tillate å installere eiga programvare for behandling av personopplysingar.

Leverandørar og partnerar

- Leverandørar og partnerar skal vere godkjente av organisasjonen. Dette skal skje gjennom innkjøpsavtalar og databehandlaravtalar.

Innkjøp av hardware og software

- Ved innkjøp av hardware og software skal alltid IT-leiar vurdere teknologiske spørsmål før innkjøpet skjer.

Heimekontorløysingar

- Alle som nyttar heimekontorløysing på open sone skal sikrast med teknisk sikkerheit i løysinga og etter policy for heimekontor.

4.3 Ansvar for etterleving av sikkerheits-mål og strategi

Kommunen og alle tilsette skal arbeide slik at sikkerheits-måla og strategien blir etterlevd. Det overordna føremålet med behandling av personopplysningar er å sikre den registrerte sine rettar og hindre at personvernet vert krenka. Kven som har ansvar for kva når det gjeld personvern og informasjonssikkerheit, er forklart i kapittelet om sikkerheitsorganisasjon og ansvar.

5. Sikkerheitsorganisasjon og ansvar

Arbeidet med personvern og informasjonssikkerheit skal ha ein forankring i leiinga i kommunen. Kommunen sin behandlingsansvarleg er kommunedirektøren, som har ansvaret for at regelverk vert overheldt og skal sørgje for at krav til personvern og informasjonssikkerheit vert følgt og innarbeidd i avtalar med tilsette, partnarar, leverandørar og andre det blir utveksla informasjon med. Dette skal skje i form av databrukaravtalar og databehandlaravtalar.

Tilsette skal praktisere og etterleve personopplysningslova og GDPR-forordninga gjennom organisasjonen sin overordna plan for personvern og informasjonssikkerheit og gjeldande prosedyrar.

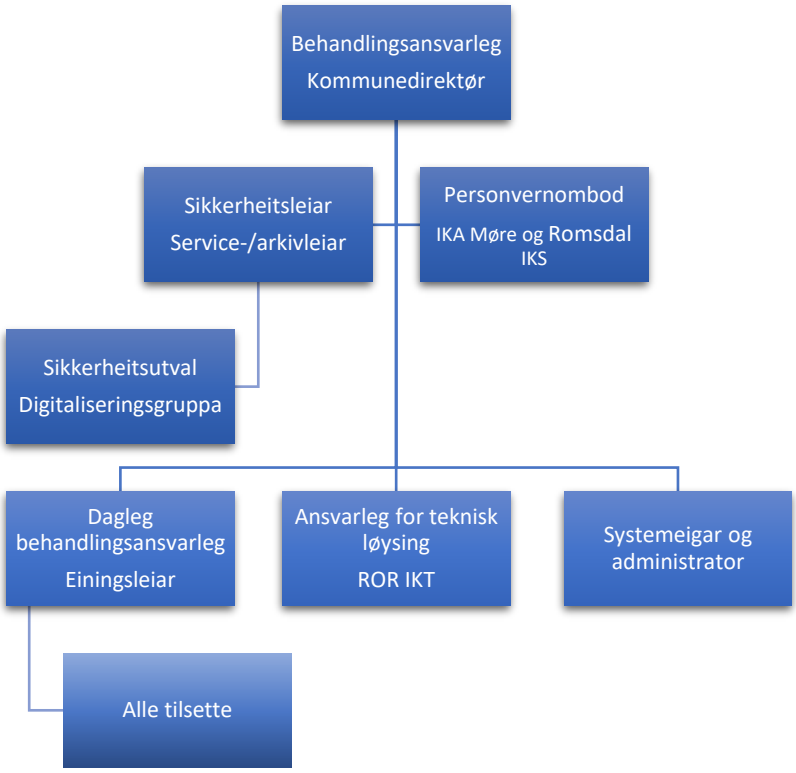
Systemeigar skal forvalte og beskytte dei verdiar som systemet representerer, dvs. at funksjonaliteten til systemet vert vareteke på ein tilfredsstillande måte.

Alle tilsette skal setje seg inn i relevante planer og prosedyrar som set ramme for bruk og oppbevaring av informasjon.

5.1 Sikkerheitsorganisasjonen

I kommunen er det lagt vekt på at arbeidet med informasjonssystema skal vere av ein slik karakter at sikkerheit i forhold til integritet, tilgjengelegheit og konfidensialitet vert vareteke.

Leiinga i kommunen har forankra dette i organisasjonen på ein slik måte at nødvendig fokus frå leiarane vert vareteke.



5.2 Ansvarsfordeling

Oversikt over oppgåver som ligg til rollene, er beskrive i prosedyren «Organisasjonskart – sikkerhetsorganisasjon» som ligg i kommunen sitt kvalitetssystem.

5.2.1 Behandlingsansvarleg (kommunedirektøren)

Kommunedirektøren er behandlingsansvarleg og har det overordna ansvaret for at kommunen følgjer dei krav som gjeld for tilfredsstillande informasjonssikkerheit etter personopplysningslova og andre relevante lover og forskrifter. Kommunedirektøren skal organisere ansvar, roller og oppgåver innanfor arbeidet med informasjonssikkerheita.

Ansvarsområde:

- Fastsetje krav til sikkerheitsmål og -strategi for informasjonsbehandling i organisasjonen.
- Velje sikkerheitsleiar og medlemer til eit sikkerheitsutval (dersom dette blir nytta).
- Velje personvernombod og blant anna:
    - stille til råderett dei ressursane som er nødvendige for å utføre lovpålagde oppgåver og opprettholde sin kunnskap.
    - sikre at personvernombodet på riktig måte og i rett tid blir involvert i alle spørsmål som gjeld vern av personopplysingar.
    - gi tilgang til personopplysingar og behandlingsaktivitetar.
    - sikre at personvernombodet er uavhengig og ikkje mottek instruksar om utføringa av oppgåvene sine.
    - sikre at personvernombodet ikkje vert avsett eller blir straffa for å utføre oppgåvene sine.
    - sørgje for at personvernombodet er bunde av teieplikt.
    - at personvernombodet sine kontaktopplysingar blir gjorde kjend for tilsett/dei registrerte og tilsynsstyresmakta (Datatilsynet).
- Sørgje for at organisasjonen gjennomfører nødvendige tryggingstiltak i samsvar med overordna krav og retningslinjer.
- Sørgje for at informasjonstryggleik er klart og eintydig definert og at forholda lagde til rette for gjennomføring.
- Lage mål og strategiplanar for informasjonstryggleik.
- Initiere leiinga sin gjennomgang av informasjonsvernet minimum ein gong i året.
- Sikkerheitsrevisjon:
    - Kartlegging av risikoområde knytte til personvern og informasjonssikkerheit.
    - Revisjon av prosedyrar for personvern og informasjonssikkerheit.
- Sikre at informasjonstryggleik blir drøft i eige fora.

5.2.2 Personvernombod

- Informere og gi råd til dei behandlingsansvarlege, tilsett og databehandlar om pliktar dei har etter regelverket om personopplysingar.
- Kontrollere etterleving av regelverket, medrekna fordeling av ansvar, haldningsskapande tiltak og opplæring av personellet som utfører behandlingsaktivitetar og revisjon.
- På oppmoding gi råd om vurdering av personvernkonsekvensar og kontrollere gjennomføring der dette er påkrevd.
- Gjennomføre førehandsdrøftingar der dette er påkrevd.
- Samarbeid med og vere kontaktpunktet for tilsynsstyresmakt (Datatilsynet)
- Vere kontaktpunktet for dei registrerte i alle spørsmål som omhandlar behandling av personopplysingane deira.
- Bunde av teieplikt eller ei plikt til konfidensiell behandling av opplysingar.

- Personvernombodet kan i tillegg til dette ha andre oppgåver, så lenge det ikkje fører til interessekonfliktar.

5.2.3 Sikkerheitsansvarleg

Denne rolla er lagt til serviceleiar. Sikkerheitsansvarleg har eit overordna operativt ansvar. Sikkerheitsansvarleg har mynde til å pålegge einingsleiar ansvar når det gjeld ulike oppgåver innanfor området informasjonssikkerheit og har kontrollansvaret i kommunen. Sikkerheitsansvarleg leiar også kommunen si beredskapsgruppe innan dette området. Sikkerheitsansvarleg rapporterer direkte til kommunedirektøren.

Ansvarsområde:

- Sikre at dagleg ansvarleg (tenesteområdeleiar) gjennomfører pålagte oppgåver knytt til personvern og informasjonssikkerheit.
- Sørge for at sikkerheitsmål og -strategi vert etterlevd.
- Sørge for at system for internkontroll følgjer krava etter personopplysningsloven.
- Rapportere alvorlege brot på reglar om behandling av personopplysningar til rådmann og eventuelt Datatilsynet.
- Sørge for at det vert gjennomført revisjonar av sikkerheitsarbeidet.
- Utarbeide rapport til leiinga si årlege gjennomgang.
- Gjennomføre leiinga sin gjennomgang.
- Ansvar for å revidere kommunen sine prosedyrar for personvern og informasjonssikkerheit.
- Sørge for at opplæring i informasjonssikkerheit og fagsystem gjennomførast i eigen organisasjon.

5.2.4 Sikkerheitsutval

Kommunens digitaliseringsutval er også kommunens sikkerheitsutval, der det vert gjeve gjensidig informasjon til partane og det skal arbeidast med forbetring av kvaliteten på dette området. Utvalet er leia av sikkerheitsansvarleg.

5.2.5 Dagleg behandlingsansvarleg (tenesteområdeleiar)

Tenesteområdeleiar har ansvaret for tilfredsstillande personvern og informasjonssikkerheit i eiga eining. Einingsleiar rapporterer direkte til behandlingsansvarleg og sikkerheitsansvarleg.

Ansvarsområde:

- Er dagleg ansvarleg for sikker behandling av personopplysningar i eiga eining.
- Informere dei tilsette om sikkerheitsprosedyrar og sørge for at desse vert følgt.
- Sørge for
    - opplæring i informasjonssikkerheit og fagsystem i eiga eining,
    - at internkontrollsystemet blir brukt
    - føring av behandlingsprotokoll
    - etterleving av prosedyrane for informasjonssikkerheit og personvern,
    - gjennomføring personvernkonsekvensvurdering.
    - at lokala er sikra på ein forsvarleg måte, slik at uvedkommande ikkje får tilgang til personopplysningar.
    - at det blir gjennomført risikovurderingar.
    - gjennomføring og dokumentasjon av eigenkontroll.
- Behandle meldte avvik i tråd med gjeldande prosedyrar.
- Melde behov for forbetring/endring av gjeldande prosedyrar.
- Sikre at tilsette har rette tilgangar:

    - Ha oversikt over og ta avgjerder om autorisert bruk.
    - Bestemme tilgangar til system/nivå/funksjonar.
- Leiar sikrar personopplysningar ved:
    - At personopplysningar blir delt med medarbeidarane som har bruk for informasjonen i arbeidet sitt.
    - At den enkelte medarbeidar får forholda lagt til rette slik at vedkommande kan ta i vare sitt personlege sikkerheitsansvar.

5.2.6 Ansvarleg for teknisk løysing

ROR IKT har i oppgåve å drifte og sikre den tekniske løysinga i Rauma kommune. ROR IKT har mynde til å pålegge einingsleiar ansvar når det gjeld ulike oppgåver når det gjeld informasjonssikkerheit innanfor it-teknikaren sine arbeidsområde. Ansvarleg for teknisk løysing rapporterer direkte til kommunedirektøren eller sikkerheitsansvarleg i Rauma kommune.

Behandlingsansvarleg har ansvar for å utarbeide ein beredskapsplan for å sikre at driftskritiske datasystem er operative dersom det skulle oppstå hendingar (straumbrot, flaum, brann, hærverk, sabotasje med meir).

Ansvarsområde:

- Utarbeide ein driftsdokumentasjon for IT-drift av kommunen sine lokale løysingar.
- Utarbeide system for IT-drift.
- Ved ekstern driftspartnar på IT-drift skal samarbeidsforholdet regulerast gjennom databehandlaravtale og driftsavtale.
- Avslutte brukarkonto ved opphøyr av arbeidsforhold.

5.2.7 Arkivleiar

Arkivleiaren har det faglege ansvaret for arkivområdet i kommunen. Arkivleiaren er organisert i service- og dokumentsenteret og rapporterer direkte til sikkerheitsansvarleg. For tida er sikkerheitsleiar også service- og arkivleiar.

Ansvarsområde:

- Sørge for
    - opplæring i informasjonssikkerheit og fagsystem i eiga eining.
    - at internkontrollsystemet blir brukt.
    - at lokala er sikra på ein forsvarleg måte, slik at uvedkommande ikkje får tilgang til personopplysningar lagra i arkiv.
    - at det blir gjennomført risikovurderingar for arkiv.
    - at dokumentasjonsstrategien er oppdatert.
    - data og dokumentasjon vert klassifisert og lagra etter gjeldande retningsliner.
    - eigenkontroll vert gjennomført og dokumentert.
- Hjelpe med avklaringar omkring arkivformålet; «Allmennhetens interesse, forskning - vitenskapelig, historisk og statistikk. (PVF art 89 nr 1) - annet (personopplysninger som fortjener et sterkere vern)».
- Hjelpe etter behov ved alle førespurnader når det gjeld den registrerte sine rettar.

Oversikt over dei enkelte prosedyrane og ansvarsforholda kring desse, er skildra i vedlegg 2.

5.2.8 Systemeigar

- Overordna juridisk ansvar for fagsystema.

- Overordna ansvar for at det er økonomisk dekning for alle utgifter knytt til systemet inklusive oppdatering og opplæring.
- Dagleg ansvar for å oppfylle plikter som behandlingsansvarleg på vegne av kommunedirektøren.
- Ansvar for å utnemne systemansvarleg.
- Overordna ansvar for å gi eigne brukarar nødvendig opplæring i systemet.
- Fullmakt til å bestille tilbakeføring (recovery) av data tilhøyrande fagsystemet.
- Ansvar for best mogeleg utnytting av systemet.

5.2.9 Systemansvarleg/systemadministrator

- Systemansvarleg har fagleg ansvar for bruk og administrasjon av systemet og blir vald av tenestemottakaren sin systemeigar.
- Systemansvarleg har det daglege forvaltingsansvaret for systemet og skal gjennom systemeigar sine retningslinjer sikre at systemet er levedyktig og oppdatert, og har tilfredsstillande informasjonssikkerheit.
- Systemansvarleg skal også sørge for at lover og forskrifter vert etterlevd i praksis.
- Etablere og dokumentere rutinar for vedlikehald og utlevering av brukartilgangar.
- Etablere og dokumentere rutinar som er nødvendige i forhold til bruk av systemet.
- Etablere og dokumentere rutinar for sikker tenesteyting ved mellombels systembortfall.

6. ROS og DPIA

ROS = Risikoanalyse
DPIA: Personvernkonsekvensvurdering

6.1 Risikoanalyse (ROS) – internkontroll i praksis

6.1.1 Truslar og farar

Som ein del av internkontrollen skal kommunen ha ei oversikt over kva behandling av personopplysingar organisasjonen har (behandlingsprotokoll, jf. kap. 2.3 i styringsdokumentet), og kva personopplysingar som inngår i desse. Denne oversikta skal brukast som underlag ved risikovurderingar. I tillegg må kommunen ha kunnskap truslar og farar, både internt i organisasjonen og utanfor organisasjonen, og tilpasse seg dette.

Kommunen kan ikkje forme trusselen, men det er mykje den kan gjere for å tilpasse seg den. Å tilpasse trusselbildet kan kommunen gjere ved å gjennomføre ei risikovurdering- og analyse av aktuelle trusselbilde.

6.1.2 Risikovurdering- og analyse

Risikovurdering er ei grunnleggjande del av sikkerheitsarbeidet. I samband med informasjonssikkerheit fortel risiko kva som er mulegheita for å lide tap eller bli påført skade ved eit gitt sikkerheitsbrot.

Ei risikovurdering er eit verktøy for å identifisere uønskte hendingar og risikoen for at desse skal hende. Risiko har to dimensjonar: skadeverknad (konsekvens av eit sikkerheitsbrot hender) og sårbarheit (sannsynlegheit for at eit sikkerheitsbrot hender).

Risikovurderinga må sjåast i samanheng med etablert akseptkriterium for risiko, og den behandlingsansvarlege skal setje i verk nødvendige tiltak for å oppnå tilfredsstillande informasjonssikkerheit.

6.1.3 Når skal kommunen gjennomføre ROS?

- Kommunen skal gjennomføre overordna risikoanalysar for kommunen og for alle einingane for å oppnå tilfredsstillande informasjonssikkerheit.
- Kommunen skal gjennomføre risikovurdering før ein sett i verk ei behandling av informasjon og før ein tek i bruk eit informasjonssystem.
- Kommunen skal vidare gjennomføre risikovurdering ved endringar i forhold som kan påverke informasjonssikkerheita, for eksempel endringar i behandlingar av informasjon, endringar av informasjonssystem eller endringar i trusselbiletet.
- Kommunen skal gjennomføre ROS-analyser for alle fagsystem, identifisere risiko og gjennomføre risikoreduserande tiltak.

6.2 Personvernkonsekvensvurdering (DPIA)

Kommunen skal gjennomføre ei vurdering av personkonsekvensar for å vurdere kor stor risiko for dei registrerte sitt personvern behandlingsaktiviteten fører med seg. Er risikoen høg, kan dette føre til at behandlingsaktiviteten må stoppe. Mal for DPIA er lagra i kommunens saks- og arkivsystem.

6.2.1 Når skal behandlingsansvarleg gjennomføre ein DPIA?

Vurderinga av om det skal gjennomførast ein DPIA er berre obligatorisk dersom behandlinga av personopplysningar sannsynlegvis medfører ein høg risiko for dei fysiske personane sine rettar og fridomar. Også i tilfelle der det ikkje er høg risiko for brot på personvern, blir det råda til å utføre ein personvernkonsekvensanalyse.

6.2.2 Når er det ikkje nødvendig med eit DPIA?

Det treng ikkje gjennomføre ein DPIA dersom behandlinga sin art, omfang, samanheng og formål er veldig lik ei tidlegare behandling som det allereie er utført DPIA for eller dersom behandlinga tidlegare har fått konsesjon frå Datatilsynet gjennom den tidlegare ordninga.

6.2.3 Når skal det gjennomførast førehandsdrøfting med Datatilsynet?

Det er nødvendig med ei førehandsdrøfting når behandlingsansvarleg har gjennomført ei vurdering av personvernkonsekvensar og behandlinga framleis medfører høg risiko for rettar og fridomar for dei registrerte.

Når den behandlingsansvarlege ikkje kan finne tilstrekkelege tiltak for å avgrense risikoen til eit akseptabelt nivå (det vil seie at restrisikoen framleis er høg), er det krav om førehandsdrøfting med Datatilsynet. Dette betyr då at behandlinga har framleis høg risiko ved at den kan ha høg innverknad, inngripen eller krenking av personvernet til dei registrerte, eller dei registrerte sine rettar og fridomar. Og at denne risikoen ikkje kan reduserast.

Den behandlingsansvarlege må også rådføre seg med Datatilsynet når det er eit krav i lova at den behandlingsansvarlege skal rådføre seg med, og innhente førehandsgodkjenning frå Datatilsynet, i samband med ei oppgåve som blir utført av eit behandlingsansvarleg i «allmennhetens interesse», knytt til sosial tryggleik og folkehelse (jf. personvernforordninga artikkel 36 nr. 5).

6.2.4 Ansvarleg for gjennomføring av DPIA

- Behandlingsansvarleg skal sikre at det vert gjennomført ein DPIA.
- Sikkerheitsansvarleg skal gje leiarane kunnskap om DPIA og når dette skal gjerast.
- Personvernombodet skal hjelpe til med gjennomføringa
- Leiar skal delta i DPIA

Dersom det vert starta ein behandling av personopplysningar der DPIA ikkje er vurdert gjennomført, er dette å rekne som avvik som skal meldast i kommunen sitt avvikssystem.

7. Prosedyrar

Det er utarbeidd eit sett med prosedyrar som beskriv nærare korleis organisasjonen og tilsette kan oppfylle sentrale krav til forsvarleg informasjonssikkerheit. Desse prosedyrane er lagra i Rauma kommune sitt kvalitetssystem; «IK/HMS». Prosedyrane skal danne grunnlaget for arbeidet med informasjonssikkerheit i kommunen og skal til ein kvar tid vere oppdatert.

Kommunedirektøren er behandlingsansvarleg og legg grunnlaget for arbeidet gjennom styrande prosedyrar og overordna dokument. Leiarane er behandlingsansvarleg på eigne område og har ansvaret for at tilsette har kunnskap om og følgjer retningslinjene og prosedyrane for handtering av informasjonssikkerheit.

Formålet med prosedyrar for dagleg informasjonssikkerheit er at den einskilde medarbeidaren utfører daglege rutinar/handlingar/aktivitetar slik at det varetek den daglege informasjonssikkerheita på ein tilfredsstillande måte.

Dagleg informasjonssikkerheit gjeld alle tilsette som behandlar informasjon elektronisk eller skriftleg, som inneheld gradert eller sensitiv informasjon og/eller stiller krav til fysisk sikring for å hindre uautorisert tilgang til desse systema/informasjonen.

Prosedyrane er delt inn i 3 kategoriar der ulike roller har ulikt ansvar for etterleving. Gjennomførande prosedyrar inneheld også administrative og daglege prosedyrar.

Prosedyrane er delt inn slik med definerte ansvarlege under:

Styrande	Kontrollerande	Gjennomførande	Administrative	Daglege
•Behandlings-ansvarleg •Sikkerheits-ansvarleg •Leiar •Alle tilsette	•Behandlings-ansvarleg •Sikkerheits-ansvarleg •Personvern-ombod •Leiar	•Behandlings-ansvarleg •Sikkerheits-ansvarleg •Personvern-ombod •Leiar •Alle tilsette •Arkivleiar •Systemeigar •Systemansv.	•Behandlings-ansvarleg •Sikkerheits-ansvarleg •Personvern-ombod •Leiar •Alle tilsette •Arkivleiar •Systemeigar •Systemansv.	•Alle

Oversikt over kva typar prosedyrar kommunen skal etablere, er omtala i vedlegg 2.

8. Eigenkontroll

Leiar skal gjennomføre årleg kontroll av dagens situasjon og gjennomgang av prosedyrar og aktivitetar knytt til personvern og informasjonssikkerheit.

Leiar skal vere kjent med dei ulike prosedyrane og oppgåvene som ligg til leiarrolla. Kommunen har etablert ei sjekkliste for gjennomføring av eigenkontroll, som leiarane skal bruke i sitt arbeid med eigenkontrollen.

Skjemaet skal sendast til sikkerheitsleiar etter gitte fristar, og vert ein del av leiinga sin årlege gjennomgang av status i arbeidet med personvern og informasjonssikkerheit.

9. Leiinga sin gjennomgang

9.1 Føremål

Leiinga skal vurdere status for sikkerheita i behandling av personopplysingar i kommunen. Gjennomgangen skal også omfatte korleis kommunen har teke i vare informasjonssikkerheita generelt (t.d. kva fysiske sikringstiltak er iverksett, kva organisatoriske tiltak som er gjennomført for å sikre at tilsette følgjer kommunen sine prosedyrar for informasjonssikkerheit. Vidare skal gjennomgangen danne grunnlag for nødvendig revisjon av sikkerheitsmål og strategi.

9.2 Ansvar

Sikkerheitsleiar har ansvaret for å kalle inn til minimum eit møte i året og legge fram resultat frå eigenkontrollen. Ved behov skal det gjennomførast oftare møter.

Leiinga sin gjennomgang skal skje etter PDCA-prinsippet, som er omtala i styringsdokumentet kap. 2.4.1.

9.3 Aktivitet

Følgjande skal gjennomgåast ved leiinga sin gjennomgang:

- Resultat frå eigenkontroll og kontroller utført av offentlege myndigheiter
- Endringar av verdi for drift av informasjonssystemet eller for informasjonssikkerheita.
- Endringar i offentlege sikkerheitskrav.
- Endring i dei personopplysingane organisasjonen behandlar.
- Endringar i trusselbiletet som blant anna skildra i rapporten frå utførte risikoanalysar.
- Om informasjonssystemet bør endrast, eksempelvis som følgje av ønske om ny funksjonalitet eller utvida bruk.
- Leiinga skal årleg gå gjennom sikkerheitsmåla og strategien, samt organiseringa av informasjonssystemet. Leiinga skal kontrollere at desse er i samsvar med organisasjonen sitt behov.
- Gjennomgang av hendingar og avvik

9.4 Forbetringstiltak

Forbetringstiltak skal utarbeidast frå ei samla vurdering av kommunens sikkerheitsmål, rapporterte hendingar, avvik, forbetringsforslag, og eigenkontrollar. Anbefalte forbetringstiltak vert presentert i prioritert rekkefølgje innanfor kvart av desse områda:

- Sikkerheitsorganisasjon
- Personsikkerheit
- Fysisk sikring
- Dokumentsikkerheit
- Systemteknisk sikkerheit
- Driftssikkerheit/-beredskap

9.5 Oppfølging

Leiinga fattar eit vedtak i form av oppfølgingspunktar. Desse punkta skal vektleggjast i einingane sin eigenkontroll fram til neste leiinga sin gjennomgang. Leiinga fattar vedtak om eigenkontroll.

9.6 Referat

Leiinga si gjennomgang skal dokumenterast i form av eit referat og rapport frå sjølve gjennomgangen. I referatet skal det tydeleg gå fram dei tiltaka som er vedteke med ei grunngjevnad, samt ansvar og fristar for gjennomføring av tiltak. Gjennomgangen skal arkiverast i kommunens saks- og arkivsystem.

10. Beredskap

10.1 Generelt

Kommunen må vere førebudd på uforutsette hendingar og ekstraordinære situasjonar. Kommunen må ha lagt planar, og sørgje for å ha nødvendig personell med tilstrekkeleg opplæring og utstyr tilgjengeleg på kort varsel i tilfelle det ekstraordinære inntreff.

Ein viktig del av opplæringa er å øve på bruk av desse planane. Dette bør skje minst ein gong i året. Erfaringar frå øvingar må brukast til å forbetre planane. Den digitale beredskapen fortel kor godt ein organisasjon er i stand til å handtere det uventa.

Ein del av god førebygging er å vere førebudd på å handtere det uventa. Undersøkinga *Bruk av IKT i* staten19 for 2014 viser at sjølv om 73 prosent av verksemdene har etablert ein beredskapsplan er det berre 29 prosent som gjennomfører årlege beredskapsøvingar.

Medverknad i risikovurderingar og øvingar er viktig for å auke forståinga for risiko, og det er avgjerande at dei som eig risikoen deltek i slike aktivitetar. Øvingar gir erfaring i å handtere utfordrande situasjonar i forhold til sikkerheit og avdekkjer eventuelle svakheiter i beredskapsplanane.

Eksempel på hendingar som kan medføre risiko:

- Fysiske brot på sikkerheita (uvedkommande sin tilgang til sensitiv informasjon)
- Skadar på utstyr, serverar ved brann eller vasskadar
- Brot på straumforsyning
- Klimatiske forhold i serverrom
- Virus og datakriminalitet (hacking)
- Bruk eksterne lagringsmedium som minnepinnar, berbare PC-ar, mobiltelefonar.

10.2 Målsetjing for beredskapsarbeidet

Kritiske funksjonar skal vere identifisert og dokumentert i ei beredskapsplan, og ansvarsforhold skal klarleggast. Beredskapsplanen skal vere ein del av internkontrollen og eigenkontrollen i heile organisasjonen.

Talet på einingar som årleg øver IKT-beredskap skal auke. Den enkelte eining bør sjølv vektleggje å gjennomføre årlege øvingar med klare mål knytt til informasjonssikkerheit.

Vidare er det ei målsetjing at talet på einingar som har oppdaterte IKT-beredskapsplanar skal auke.

10.3 Innhaldet i ein beredskapsplan

Beredskapsplanen må som eit minimum innehalde:

- Ansvar og handtering av hendingar skal være avklart i eit organisasjonskart.
- Einingane skal ha ein plan for korleis dei skal drifte tenesta i ein situasjon der IKT-infrastruktur ikkje er tilgjengeleg på kort og lang sikt, i verste fall over fleire dagar og veker.
- Effektiv handtering av hendingar skal sikrast gjennom rutinar som er tilgjengeleg for relevante personar.
- Varslingsrutinar skal eksistere der både relevant personell i kommunen, IT-avdeling og andre relevante partnerar inngår.
- Informasjon om at hendingar skal meldast som avvik i kommunens kvalitetssystem.

- Drift og plan for å gjenopprette normaldrift skal vere tilgjengeleg for relevante personar.

10.4 Beredskapsorganisasjon

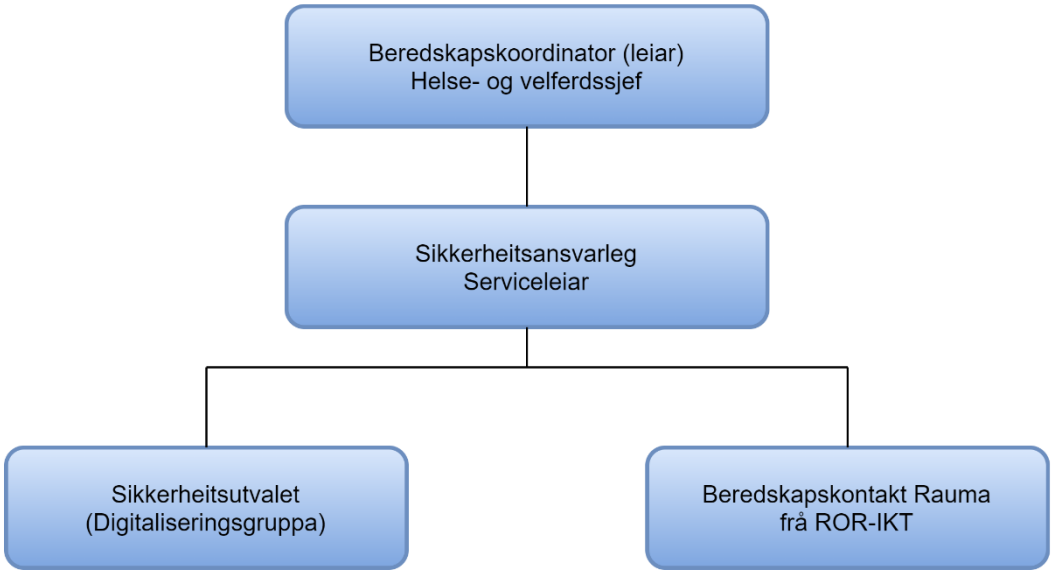
ROR-IKT er kommunen sin IKT-avdeling, også i beredskapssituasjonar. I ein beredskapssituasjon stiller ROR-IKT med ein representant (IKT-koordinator) i kommunen sin beredskapsorganisasjon, som også vert kommunen sin kontaktperson. I tillegg etablerer ROR-IKT sin eigen stab i forhold til omfang og behov, jf. organisasjonskartet nedanfor.

ROR IKT er organisert med ein operativ leiar som er direkte kontaktperson for IKT-koordinator som sit i beredskapsorganisasjonen. Operativ leiar skal ha oversikt og tilgang til ROR-IKT sin operative organisasjon og har ansvar for å gje ressursar internt i ROR-IKT for å dekkje dei behova som er oppstått.

Dagleg leiar er øvste leiar i ROR-IKT også i ein beredskapssituasjon, og er då eit naturleg eskaleringspunkt i dei situasjonane ein kjenner behov for dette. Dette gjeld både for ROR-IKT og også for kommunen sin beredskapsorganisasjon.

Beredskapskontakten frå ROR-IKT vert kalla inn til møte i Rauma kommune sin kriseleiing ved behov.

10.4.1 Rauma kommune sin beredskapsorganisasjon for informasjonssikkerheit og IKT



11. Kunnskap, kompetanse og kultur

Kommunen skal styrke den interne kunnskapen, kompetansen og kulturen innan informasjonssikkerheit i alle ledd i organisasjonen, og den totale sikkerheitskulturen i kommunen skal styrkast.

11.1 Interne truslar versus personellsikkerheit

I organisasjonen er det ulike trusselaktørar som kan gjere oss sårbare. Å bruke ordet «truslar» kan bli oppfatta negativt, så vi har valt å kalle intern trussel for personellsikkerheit. Både teknologiske og sosiale tiltak må setjast i verk for å handtere dette, jf. kap. 1.2 i styringsdokumentet.

- Teknologiske tiltak: Videoovervaking, tilgangskontroll med meir.
- Sosiale tiltak: Opplæring, varslingskanalar, melde avvik, leiaropplæring, teieplikt og årlege sikkerheitssamtalar.

11.2 Leiing og personellsikkerheit

Personellsikkerheit krev ulik leiaråtferd alt etter kva situasjon leiaren er i. I ein situasjon der ein skal tilsetje nye medarbeidarar, kan ikkje leiar gje ut så mykje informasjon om organisasjonen som ein tilsett har tilgang til. Når ein tilsett sluttar, bør leiar snakke om kva informasjon den tilsette ikkje kan bringe vidare og kvifor. Leiar bør også minne om teieplikta som den tilsette signerte ved starten av arbeidsforholdet.

11.3 Tiltak for å styrke kunnskap, kompetanse og sikkerheitskultur innanfor personvern og informasjonssikkerheit

I sikkerheitsorganisasjonen er det beskrive kva oppgåver som ligg til den enkelte tilsette ut frå roller i organisasjonen.

Det å skape ein felles forståing av risiko og utvikle ein god sikkerheitskultur i organisasjonen er utfordrande, ressurskrevjande og vil ta tid. Den tilsette må få tilført tilstrekkeleg kunnskap og kompetanse om informasjonssikkerheit på sitt fagområde for å kunne utføre sitt arbeid på ein trygg og sikker måte, som er i tråd med gjeldande plan og prosedyrar.

Det er den enkelte leiar som har ansvaret for å sikre at tilsette har tilstrekkeleg kompetanse og legge til rette for at tilsette får den nødvendige kunnskapen. Einingane må ha jamleg fokus på informasjonssikkerheit gjennom året. Dette vil danne grunnlaget for sikkerheitskulturen i kommunen.

For å auke kunnskap, kompetanse og forbetre sikkerheitskulturen innanfor arbeidet med informasjonssikkerheit og personvern, skal kommunen:

- Organisere og legge til rette for informasjonsdeling i einingane og mellom einingane
  - Arena for kompetansedeling mellom einingane er mellom anna sikkerheitsutvalet.
- Leggje til rette for felles tiltak for å styrkje sikkerheitskulturen i organisasjonen, som til dømes e-læringsprogram og kampanjar
  - «Nasjonal sikkerhetsmåned»
  - Bruke e-læringsprogram til opplæring (for eksempel KS Læring)
- Hente ut status frå einingane på deira arbeid med opplæring og sikkerheitskultur
- Leiarane:
  - har hovudansvaret for opplæring av sine tilsette, samt førebygge og avdekke ulike truslar mot personvernet og informasjonssikkerheita.

        - Mellomleiarar/avdelingsleiarar bør delta i dette arbeidet saman med leiar.
    - Leiarane må ha kompetanse i å gjennomføre sikkerheitssamtaler med sine tilsette årleg.
    - Leiar må vurdere kva kompetanse den tilsette treng å ha, samt kva informasjon dei må ha tilgang til (tenestleg behov).
    - Leiarane må ha spesielt fokus på personellsikkerheit ved omorganiseringar (endringar i tilgangsstyring?), når tilsette sluttar og kva informasjon ein gjer i en tilsetjingsprosess.

12. Overføring av opplysningar til utlandet

I utgangspunktet er det ikkje lov å overføre personopplysingar til land utanfor EØS. Det finst likevel nokre unnatak frå denne regelen, typisk ulike ordningar der den som mottek opplysingane i tredjeland (dataimportøren) tek på seg bestemde plikter. Slike ordningar kallas overføringsgrunnlag. Dersom behandlingsansvarleg skal overføre personopplysingar til eit land utanfor EØS, må behandlingsansvarleg først ha eit passande overføringsgrunnlag samt oppfylle tilleggskrava som EU-domstolen har sett.

Meininga med overføringsgrunnlaget er å gi dataimportøren ei rekkje plikter for å sikre at europearane sine personopplysingar blir like godt beskytta etter overføringa til tredjeland som dei blir i EØS. Dataimportøren kan likevel vere underlagt lokale lover som er i strid med og går føre pliktene etter overføringsgrunnlaget, eller det kan vere andre forhold som reduserer beskyttelses-nivået.

Behandlingsansvarleg må derfor først undersøkje om beskyttelse av opplysningane som vert overført, faktisk vert beskytta etter EØS-nivået og personvernforordninga. Her er det blant anna særleg viktig å undersøkje om det finst overvakingslover eller andre lover som gir myndigheitene i tredjeland urimeleg stort tilgjenge til data, samt om rettane til den registrerte vert teke i vare.

Behandlingsansvarleg kan overføre personopplysingar i land tilhøyrande EØS, altså EU-landa samt Noreg, Island og Liechtenstein, utan å tenkje på overføringsgrunnlag og tilleggskrava til EU-domstolen. Det same gjeld land og område godkjent av EU-kommisjonen. Per i dag er følgjande land og område godkjente: Andorra, Argentina, Canada (gjeld ikkje dersom mottakaren er eit offentleg organ), Færøyane, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Sveits og Uruguay. Vi kan også sende opplysningar til Storbritannia sjølv om dei ikkje lenger er medlemmar av EU.

Vedlegg 1 Personvern og informasjonssikkerheit

1. Kva er personvern?

Personvern skal gje beskyttelse av privatlivets fred. Organisasjonen må vere open om kva for teknologi som blir nytta og kva den blir nytta til. Personar har rett på ein privat sfære som vi sjølv skal kunne kontrollere. Dette må ligge til grunn ved bruk og utnytting av informasjonsteknologi. Ytringsfrihetskommisjonen (NOU 1999:27) har sagt:

> *«Den private sfæren, eller intimsfæren, er sfæren der man omgås dem man kjenner. Det er, og bør være, en frihetssfære i den forstand at den i omfattende grad er beskyttet mot reguleringer og inngrep fra offentlige (…)»*

§ 102 i grunnlova (ny § I 2014) seier mellom anna noko om at ein kvar har rett til respekt for sitt privatliv og sin kommunikasjon. Lova skal sikre eit vern om den personlege integriteten. Retten til privatliv og retten til å bestemme over eigne opplysningar er ein sentral del av personvernet.

1.1 Personopplysningar

Personvernforordningen artikkel 4:

> *«Personopplysninger er «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet»*

Personopplysning er opplysingar eller vurderingar som kan knyttas til ein enkeltperson. Dette kan vere namn, adresse, telefonnummer, e-postadresse, bilnummer, bilete eller fødselsdato.

Personprofil: Personopplysingar som blir kombinerte og dannar grunnlag for meining om evner, åtferd, preferansar eller behov. T.d. er opplysningar om kor ein brukar bevegar seg (GPS-sporing), kor ein elev legg igjen spor etter seg i ulike informasjonssystem, ei personopplysning.

1.2 Særlege kategoriar av personopplysningar

I loven er det definert ei rekkje kategoriar av opplysningar som det skal meir til å kunne behandle enn andre opplysningar, jf. artikkel 9 i forordninga:

- opplysingar om rasemessig eller etnisk opphav.
- opplysingar om politisk oppfatning.
- opplysingar om religion.
- opplysingar om filosofisk overtyding.
- opplysingar om fagforeiningsmedlemskap.
- genetiske opplysingar.
- biometriske opplysingar med det formål å eintydig identifisere nokon.
- helseopplysningar.
- opplysingar om seksuelle forhold.
- opplysingar om seksuell legning.

1.3 Behandling av personopplysningar om straffedomar og lovbrot

Opplysingar om straffedomar og lovbrot er ikkje å rekne som særlege kategoriar av

personopplysingar, men behandling av slike opplysingar er likevel underlagt visse avgrensingar (artikkel 10).

All behandling av slike opplysningar krev eit rettsleg grunnlag etter artikkel 6 nr. 1. Det betyr at behandlingsansvarleg må ha eit lovleg rettsleg grunnlag for å kunne behandle slike opplysningar. Dersom det rettslege grunnlaget finnes i artikkel 6 nr. 1 bokstav c eller e, er det i tillegg eit krav om supplerande rettsgrunnlag i nasjonal rett (eller EU-retten).

2. Grunnleggjande personvernprinsipp (artikkel 5)

Reglane for behandling av personopplysingar byggjer på nokre grunnleggjande prinsipp. Alle som behandlar personopplysingar må opptre i samsvar med desse prinsippa, jf. personvernforordninga artikkel 5.

Dei grunnleggjande personvernprinsippa:	**Forklaring**
a) Lovleg, rettferdig og gjennomsiktige (opne)	**Lovleg:** Kommunen må ha eit rettsleg grunnlag for å kunne behandle personopplysningar. Forordninga sin artikkel 6 regulerer i kva tilfelle det er lovleg å behandle personopplysingar. Minst eitt av vilkåra i denne avgjerda må vere oppfylte for at behandlinga er tillaten. Dersom det blir behandla sensitive personopplysingar (særlege kategoriar av personopplysningar), må i tillegg minst eitt av vilkåra i artikkel 9 vere oppfylte. **Rettferdig:** Behandlinga av personopplysingar skal gjerast i respekt for den registrerte sine interesser og rimelege forventingar registrerte. Behandlinga skal dessutan vere gjennomsiktig og forståeleg for dei registrerte, den skal ikkje skje på fordekte eller manipulerande måtar. **Gjennomsiktig (ope):** Behandling av personopplysingar skal vere oversiktleg og sjølvsagd for den registrerte. Den det blir behandla opplysingar om skal vere informert om dette. Gjennomsiktigheit er med på å skape tillit og det set den registrerte i stand til å bruke rettane sine og vareta interessene sine.
b) Formålsavgrensing	Personopplysingar skal berre behandlast for spesifikke, uttrykkjelege, gitte og legitime formål. Kvart formål med behandling av personopplysingar skal identifiserast og forklarast presist. Alle formål skal vere forklarte på ein måte som gjer at den tilsette og den registrerte har same eintydige forståing av kva personopplysingane skal brukast til. At formålet skal vere legitimt inneber at det i tillegg til å ha eit rettsleg grunnlag også skal vere i samsvar med andre etiske og rettslege samfunnsnormer. Personopplysingar kan ikkje bli brukt til andre formål som ikkje er foreina med det faktiske formålet. Dersom personopplysingar skal brukast på nytt, må behandlinga anten vere lovfesta eller det må innhentast nytt samtykke. Dette krev eigne vurderingar.

c) Dataminimering	Prinsippet om dataminimering inneber å avgrense mengda innsamla personopplysingar til det som er nødvendig for å realisere innsamlingsformålet. Dersom identitetsopplysingar eller personopplysingar ikkje er nødvendige for å oppnå formålet, talar prinsippet om dataminimering i retning av å ikkje samle dei inn.
d) Riktigheit	Personopplysingar som blir behandla skal vere korrekte. Opplysingane skal også oppdaterast dersom det er nødvendig. Dette betyr at behandlingsansvarleg må sørgje for å straks slette eller rette personopplysingar som er urette med omsyn til dei formåla dei blir behandla for.
e) Lagringsavgrensing	Prinsippet om lagringsavgrensing inneber at personopplysingar skal lagrast slik at dei blir sletta eller anonymiserte når dei ikkje lengre er nødvendige for formålet dei blei innhenta for.
f) Integritet og konfidensialitet	Personopplysingar skal behandlast slik at opplysingane sin integritet og konfidensialitet vert beskytta. Det betyr at behandlinga: • Behandlinga skal ha tiltak mot uautorisert utlevering og tilgang til personopplysingar. • Behandlinga skal ha tiltak mot utilsikta og ulovleg øydelegging, tap og endringar av personopplysingar. • Behandlinga skal som standard sørgje for at personopplysingar er tilgjengelege for autoriserte personar når det er nødvendig (tilgangsstyring). • Behandlinga skal som standard sikre at personopplysingar ikkje blir gjorde tilgjengeleg for eit uavgrensa tal menneske utan den rørte personen sin medverknad. • Behandlinga skal ha tiltak for å spore endringar som blir gjorde i systemet og for å kunne handtere brot på sikkerheita. • Behandlinga skal ha tiltak for å sikre at systema som behandlar personopplysingar er robuste mot for eksempel sårbarheiter, angrep og uhell.
g) Ansvarlegheit	Prinsippet om ansvar understrekar den behandlingsansvarlege sitt ansvar for å opptre i samsvar med reglane for behandling av personopplysingar. Det er ikkje nok å berre ha ansvaret – ein må vise at ein tek ansvaret. Den behandlingsansvarlege må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket blir etterlevt til einkvar tid. Kommunen må også kunne vise at den faktisk opptrer i samsvar med reglane.

3. Kommunen sine pliktar

Etter forordninga har kommunen eit sett med plikter som skal oppfyllast. Kommunen har eigne prosedyrar for å sikre at pliktene vert varetatt på rett måte. Kommunen har følgjande plikter:

3.1 Fastsetje formål (artikkel 5)

Før kommunen set i gang med å behandle personopplysningar, må det liggje føre eit eller fleire klart formulerte formål. Kommunen kan aldri samle eller lagre personopplysningar utan eit formål. Dette vert slått fast i eit av personvernprinsippa i personvernforordninga, jf. tabell ovanfor. Personopplysningar skal berre nyttast for spesifikke, uttrykkelege, angitte og legitime formål.

3.2 Ha behandlingsgrunnlag (artikkel 6)

All behandling av personopplysingar må ha eit rettsleg grunnlag for å vere lov. Det betyr at kommunen på førehand må ha identifisert om det finnast eit behandlingsgrunnlag. Dersom det ikkje gjer det, er behandlinga ulovleg.

Kommunen må ha eit behandlingsgrunnlag for behandling av kvar enkelt personopplysing til kvart enkelt formål. Det kan berre vere eitt behandlingsgrunnlag per formål. Behandlingsansvarleg har også plikt til å informere den einskilde om kva grunnlag personopplysingane deira blir behandla på.

Aktuelle behandlingsgrunnlag:

a) Samtykke.
b) Nødvendig for å oppfylle ein avtale.
c) Nødvendig for å oppfylle ei rettsleg plikt.
d) Nødvendig for å verne vitale interesser.
e) Nødvendig for å utføre ei oppgåve i offentleg interesse eller utøve offentleg myndigheit.
f) Nødvendig for å vareta legitime interesser – interesseavveging.

3.3 Gje informasjon (artikkel 15, 12, 13 og 14)

Behandlingsansvarleg har plikt til å behandle personopplysingar på ein open måte. Dette inneber at dei må gi kort og forståeleg informasjon om korleis kommunen behandlar personopplysingane. Det blir også stilt krav til korleis kommunen skal kommunisere med dei registrerte eller enkeltpersonane.

Måtar behandlingsansvarleg skal kommunisere på:

- personvernerklæringar på heimesida,
- når brukarane/kundane skal vareta rettane sine eller
- når det skal informerast om avvik.

Behandlingsansvarleg skal kommunisere på ein kortfatta, open, forståeleg og lett tilgjengeleg måte. Språket skal vere klart og enkelt, særleg når informasjonen er spesifikt retta mot barn.

3.4 Legge til rette for rettar (kap. III)

Kommunen har plikt til å legge til rette for at den registrerte får nytte rettane sine på ein enkel måte. Les meir om den registrerte sine rettar i kapittel 2.4 i styringssystemet.

3.5 Retting og sletting (artikkel 16 og 19)

Behandlingsansvarleg har plikt til å leggje til rette for at den registrerte får vareteke rettane sine om retting og sletting. Behandlingsansvarleg har også plikt til å rette informasjon av eige tiltak.

Behandlingsansvarleg skal sørgje for at personopplysingane er av god kvalitet og er korrekte, jf. personvernprinsippa. Opplysingane skal haldast oppdaterte der det er nødvendig. Behandlingsansvarleg skal rette urette opplysingar utan opphald sjølv om den registrerte ikkje har bedt om det.

Det er forbode å oppbevare personopplysingar lenger enn det som er nødvendig for formålet dei blei samla inn for. Det vil seie at når formålet er oppfylt, skal opplysingane slettast, sjølv om dei som er registrerte ikkje har bedt om det. Behandlingsansvarleg skal ha system og rutinar som sikrar at sletting blir gjennomført.

Behandlingsansvarleg skal slette opplysingane av eige tiltak dersom behandlinga er basert på samtykke og enkeltpersonar trekkjer tilbake samtykket sitt, med mindre opplysingane samtidig blir

behandla for andre formål basert på andre behandlingsgrunnlag. Tilsvarande gjeld dersom dei som er registrerte protesterer mot behandlinga og behandlingsansvarleg må ta protesten til følgje.

Retten til å krevje sletting gjeld ikkje i følgjene tilfelle:

- Personopplysingane inngår i ei ytring som er verna av ytrings- og informasjonsfridomen.
- Lagring er nødvendig for arkivering i ålmenta sin interesse, vitskaplege eller historiske forskingsformål eller statistiske formål. Unnataket gjeld berre dersom sletting i alvorleg grad vil hindre at måla blir oppfylt. I følgje artikkel 89 skal slik behandling av personopplysingar ha tiltak og garantiar for å vareta personvernet.
- Behandlingsansvarleg har lagringsplikt etter lov (for eksempel bokføringsplikt).
- Lagring er nødvendig for visse typar bruk innan helsetenesta (etter personvernforordninga artikkel 9).
- Lagring er nødvendig for å fastsetje, gjere gjeldande eller forsvare rettskrav.

3.6 Personvernombod (artikkel 37, 38 og 39)

Behandlingsansvarleg skal ha eit personvernombod. Rauma kommune kjøper denne tenesta frå IKA Møre og Romsdal IKS.

3.7 Vurdering av personvernkonsekvensar og førehandsdrøfting (artikkel 35 og 36)

Behandlingsansvarleg er pliktig til å vurdere personvernkonsekvensar (DPIA) når dette er påkravd. I personvernforordninga artikkel 35 og 36 er det opplyst om kva tilfelle det er ein plikt å gjennomføre ein DPIA, kva den skal innehalde og kven som skal gjennomføre den. Rauma kommune skal gjennomføre DPIA i systemet Sureway (personvernappen).

Det står meir om dette i styringssystemet sitt kapittel 6.

3.8 Innebygd personvern (artikkel. 25)

Behandlingsansvarleg skal sikre at alle fagsystem/informasjonssystem inneheld ei løysing for innebygd personvern. Det betyr at desse systema oppfyller personvernprinsippa og varetek den registrerte sine rettar. Når det gjeld kva krav som skal ligge til grunn for innebygd personvern, skal kommunen bruke rettleiaren til Datatilsynet.

3.9 Informasjonssikkerheit og internkontroll

Behandlingsansvarleg skal ha eit system for internkontroll. Dette er vidare omtala i styringsdokumentet frå kapittel 3.

3.10 Behandlingsprotokollar (artikkel 30)

Behandlingsansvarleg har plikt til å føre ein protokoll over behandlingsaktivitetar som skjer i kommunen = ein oversikt over kva kommunen brukar personopplysningane til den registrerte til. Rauma kommune har eigne prosedyrar på korleis ein slik protokoll skal førast og sjølve protokollen vert utarbeidd og oppbevart i systemet Sureway (personvernappen).

3.11 Databehandlaravtale (artikkel 28 og 29)

Kommunen skal ha databehandlaravtale[4] med alle underleverandørar (databehandlar[5]) som

[4] Databehandlaravtale: Ein avtale mellom databehandlar og behandlingsansvarleg om korleis personopplysingar skal behandlast.

[5] Databehandlar: Den som behandlar personopplysingar på oppdrag frå den behandlingsansvarlege. Dette er vanlegvis ei verksemd.

behandlar personopplysningar på vegne av kommunen. Databehandlaravtalen skal sikre at personopplysningane vert behandla i samsvar med personvernforordninga og gje ei klar ramme for korleis databehandlaren kan behandle opplysningane.

Rauma kommune har ein eigen mal til databehandlaravtale som skal nyttast mot underleverandørar der det er muleg.

3.12 Avvikshandtering (artikkel 33 og 34)

Kommunen har prosedyrar som seier noko om når og korleis avvik skal meldast. Sjå meir om avvik i kapittel 2.2 i styringssystemet.

3.13 Overføring av opplysningar til utlandet (kapittel V)

Dersom kommunen sine personopplysningar vert overført til utlandet (land utanfor EU/EØS), må kommunen sikre at opplysningane vert behandla i tråd med personvernforordninga. Behandlingsansvarleg må sikre at vi har eit gyldig overføringsgrunnlag før slik overføring av opplysningar kan skje. Har ikkje behandlingsansvarlege eit gyldig overføringsgrunnlag, kan ikkje kommunen overføre slike opplysningar til andre land, jf. kap. 12 i styringsdokumentet.

4. Den registrerte sine rettar

Behandlingsansvarlege skal legge til rette for at den registrerte får oppfylt sine rettar etter forordninga kap. III. Den registrerte har medråderett over eigne opplysningar. Kommunen har plikt til å legge til rette for at den registrerte kan få oppfylt sine rettar på ein enkel måte. Den registrerte har følgjande rettar:

Den registrerte sin rett med referanse til artikkel i forordninga:	**Forklaring**
Rett til innsyn (art. 15)	Den registrerte kan be kommunen om korleis eigne opplysningar blir behandla og kva opplysningar som er lagra.
Rett til retting (art. 16)	Den registrerte kan be kommunen om å korrigere uriktige opplysningar om seg sjølv.
Rett til sletting (art. 17)	I enkelte tilfelle kan den registrerte be om at personopplysningar om seg sjølv vert sletta.
Rett til avgrensing (art. 18	Den registrerte kan be om at behandlinga av personopplysningane vert avgrensa; lagra men ikkje nyttast til noko.
Rett til å protestere (art. 21)	Den registrerte har rett til å protestere mot at personopplysningane vert behandla.
Rettar ved automatiserte avgjerder (art. 22)	Den registrerte kan krevje at avgjerder ikkje vert automatisert, men at ein saksbehandlar ser på saka.
Rett til dataportabilitet (art. 20)	Den registrerte har rett til å få utlevert personopplysningane om seg sjølv og gjenbruke desse på tvers av ulike system og tenester, t.d bytte tenesteleverandør.
Rett til informasjon (art. 13 og 14)	Kommunen har plikt til å behandle personopplysningar på ein open måte, og må gje kort og forståeleg informasjon om korleis kommunen behandlar personopplysningane.

5. Kva er informasjonssikkerheit?

Informasjonssikkerheit inneber sikringstiltak innanfor både fysiske, systemtekniske og organisatoriske område, og omfattar følgjande tre omgrep:

- **Konfidensialitet:**
  Sikkerheit for at berre autoriserte personar får tilgang til følsam eller gradert informasjon og at det på førehand er utført ei gyldig identifisering og autentisering av personen (hindre uønskt innsyn).

- **Integritet:**
  Sikkerheit for at informasjonen og informasjonsbehandlinga er fullstendig, nøyaktig og gyldig, og eit resultat av autoriserte og kontrollerte aktivitetar (beskytta mot endring/ manipulering).

- **Tilgjengelegheit:**
  Sikkerheit for at ei teneste oppfyller bestemde krav til stabilitet, slik at aktuell informasjon er tilgjengeleg ved behov (tilgjengeleg når det er ønskeleg).

Ut frå dette blir informasjonssikkerheit definert som

"sikring mot brot på konfidensialitet, integritet og tilgjengelegheit for den informasjonen som blir behandla av tilsette, systemet og systemet i seg sjølv."

6. Eit utval av relevante lover og regelsett

For å kunne regulere bruken av databehandling slik at både etiske, moralske og strafferettslege reglar i samfunnet vert ivaretekne, er det etablert ei rekkje lover, forskrifter, instruksar og myndigheitspraksis knytt til informasjonssikkerheit.

Organisasjonen skal gjennom planlagde og systematiske tiltak sørgje for tilfredsstillande informasjonssikkerheit med omsyn til konfidensialitet, integritet og tilgjengelegheit ved behandling av personopplysningar.

Alle tilsette må setje seg inn i relevante lover og reglar som set rammer for opparbeiding og oppbevaring av informasjon. Eit utdrag av relevante lovar følgjer nedanfor.

Personopplysningsloven med personvernforordninga

Lova gjeld for alle typar behandlingar etter art. 4. (1). avsnitt 2. Dette betyr lovverket regulerer korleis kommunen kan behandle personopplysingar utover tilfelle der det blir «systematisert» eller «registrert» personopplysingar.

Personopplysningslova gjeld for all offentleg og privat verksemd. Formålet med lova er å beskytte den enkelte mot at personvernet vert krenka gjennom behandling av personopplysningar ved til dømes elektronisk registrering. Lova skal bidra til at personopplysningar vert behandla i samsvar med grunnleggjande personvernomsyn, her behovet for personleg integritet, privatlivets fred og tilstrekkeleg kvalitet på personopplysningane.

Sikkerhetsloven

Lova skal førebyggje, avdekkje og motverke sikkerheitstruande verksemd. Sikkerhetsloven gjeld for statlege, fylkeskommunale og kommunale organ, samt leverandørar av varer og tenester i samband med eit hemmelegstempla innkjøp.

Arkivlova med forskrift

Arkivlova pliktar alle offentlege organ å ha arkiv, og desse skal vere organisert og sikra på ein slik måte at informasjonen kan vere tilgjengeleg som informasjonskjelde for samtid og ettertid. Det vert ikkje stilt krav til korleis arkiva bør sikrast. I arkivforskrifta er det gitt spesifikke krav til fysisk sikring av arkiv, lagringsmedium, korttids- og langtidslagring, kassasjon osv. Reglane i personopplysningslova går føre enkelte føresegner i arkivlova, jf. § 9.

Forvaltningsloven

Lova gjer generelle saksbehandlingsreglar for heile forvaltninga; kommunale, fylkeskommunale og offentlege organ. Lova inneheld reglar om vern av gradert informasjon, behandling av personopplysningar og reglar om teieplikt. Lova skal beskytte borgarane om at informasjon ikkje kjem på avveie, at borgaren vert beskytta og at opplysningane varetek omsynet til konfidensialitet og tillit.

Offentleglova

Denne lova regulerer allmennheita si rett til innsyn i dokument som organisasjonen har i hende.

Helseregisterloven

Denne lova gjeld for helsetenesta og regulerer registrering av helseopplynsingar som vert bruk til forvaltning, behandling, planlegging, forsking, statistikk med meir.

Pasientjournalloven

Denne lova regulerer utveksling av opplysningar mellom einingar innanfor helsetenesta gjennom bruk av elektronisk pasientjournal, som både skal gjere informasjon tilgjengeleg samtidig som det skal vareta omsynet til konfidensialitet.

Helsepersonelloven

Denne lova regulerer teieplikta til helsepersonell avgjerder om journal og behandling av journal.

Rett til informasjon, samtykke, medråderett og innsynsrett

Den enkelte har medråderett over eigne opplysningar krevje at opplysningar vert retta, sletta ved feil eller når opplysninga er ei belastning eller sperra for innsyn for andre.

Normen

For behandling av helseopplysningar, har Rauma kommune også forplikta seg til å bruke Normen. Normen er ein nedskriven standard for informasjonssikkerheit i helse- og omsorgstenesta for mellom anna kommunane.

Vedlegg 2

2. Oversikt over prosedyrar og ansvarsforhold

Nedanfor følgjer ei oversikt over dei ulike prosedyrane som kommunen skal etablere for å kunne ta i vare personvern og informasjonssikkerheit på ein tilfredsstillande måte. Prosedyrane er bygd opp i ulike kategoriar med ulike roller som ansvarleg, jf. Kapittel 7 Prosedyrar. Av den grunn må tilsette ha oversikt over dei ulike prosedyrane som angår deira rolle. Prosedyrane vert kontinuerleg oppdatert (enkelte av prosedyrane er på bokmål).

2.1 Styrande

- Ansvarleg for opplæring av leiarar og tilsette
- Behandlingsprotokollar – oversikt over protokollane
- Databehandlaravtale
- Fastsetting av akseptabel risiko
- Internkontrollsystem
- Personopplysningar: Rettigheitsstyring og kontroll
- Personvernerklæring
- Personvernombod: Utpeiking, kvalifikasjonar og oppgåver
- Sikkerheitsorganisasjon og ansvar
- Sikkerheitsmål og sikkerheitsstrategi
- Systemoversikt

2.2 Kontrollerande

- Eigenkontroll og sikkerheitsrevisjon
- Informasjon til dei registrerte
- Leiinga sin gjennomgang
- Oppfølging av risikovurderingar
- Opplæring personvern og informasjonssikkerheit
- Oppstart av ny behandlingsaktivitet
- Oppstart behandling av personopplysningar

2.3 Gjennomførande

- Beredskapsplanlegging
- Bruk av bærbart datautstyr
- Databehandlaravtale/ IT-driftsavtale med leverandørar SLA
- Driftsdokumentasjon
- Prosedyre for eigenkontroll
- Konfigurasjonsendringar
- Kontrolltiltak ved ekstern dataoverføring
- Fysisk sikring av vaktrom
- Teieplikt tilsette
- Teieplikt politikarar
- Teieplikt eksterne aktørar
- Behandlinga av den enkelte førespurnaden mellom verksemder
- Opprette nye brukarar på kommunens datasystem
- Prosedyre for avgrensingar i autorisasjon
- Beredskapsplanlegging

- Etablering av naudprosedyrar ved manuell drift
- Fysisk sikring av område og utstyr
- Konfigurasjonsendringar
- Lagring (arkivering) av register for hendingar
- Tilknyting via fjernaksess
- Hindre destruktiv programvare
- Adgagskort/nøklar
- Anmodning om retting/korrigering av personopplysninger
- Anmodning om begrensing av personopplysninger
- Anmodning om forespørsel/innsyn i personopplysninger
- DPIA
- Informasjonsplikt ved behandling av personopplysninger
- Innhenting av informasjon frå dei registrerte
- Innsamling av personopplysningar
- Melde avvik og avvikshandtering
- Mottak av førespurnad/anmodning om innsyn, retting, sletting av personopplysningar
- Opprettelse/sletting av brukarar på organisasjonens datasystem
- Registrere ein behandlingsprotokoll
- Rett til å behandle personopplysningar
- Tilgangsstyring til fagsystem og personopplysningar
- Unntak frå brukarens rett til å sperre helseopplysningar
- Varsling til den registrerte ved sikkerheitsbrot

2.4 Herunder daglege prosedyrar

- Arbeidsgjevar sin rett til innsyn i e-post/filer
- Bilde/video/film, e-post, internett
- Bruk av IT-utstyr og programvare
- Dei tilsette sine plikter
- Oppbevaring av personopplysningar
- Passord og skjermsperre
- Taushetsplikt og unntak fra taushetsplikt
- Telefon
- Utskift av dokument
- Bruk av apper på mobile enheter
- Identifisering
- Internpost
- Uvedkommende/besøk i lokalet

2.2 Årshjul for informasjonssikkerheit og personvern

Dette er eit utkast til årshjul for 2022. Årshjulet kjem til å endrast kvart år.

Type	Aktivitet	Mnd	Kvartal	Halvårleg
Styrande	Revidere sikkerheitsmål og strategi	Januar		
	Fastsette akseptabel risiko	Januar		
	Førebu leiinga sin gjennomgang	Januar		
	Leiarmøte oppstart av aktivitetar for denne perioden		Februar Juni September (Opplæring) November	
	Statusrapport			April September
Gjennom-førande	Gjennomgang av beredskaps-prosedyre og beredskapsplanlegging	Februar		
	Gjennomføre/oppdatere ROS, DPIA, behandlingsprotokoller og kontroll av databehandlaravtalar	Mars - August		
	Opplæring av tilsette og nytilsette i GDPR	September/ Oktober		
	Eigenkontroll	November/ Desember		
Kontrollerande	Førebu leiinga sin gjennomgang	Januar		
	Leiinga sin gjennomgang	Februar		
	Oppfølging av ROS, behandlingsprotokollar, prosedyrar og databehandlaravtalar	Februar – Mai		
	Førebu statusrapport	April August		
	Oppfølging av opplæring i personvern og informasjonssikkerheit	September/ Oktober		
	Førebu eigenkontroll	Oktober		
	Eigenkontroll og sikkerheitsrevisjon	November/ Desember		