Sikkerhetshåndbok og internkontroll

for

HATTFJELLDAL KOMMUNE

Versjon 6.0

av 10.03.2012

Innholdsfortegnelse

1. Definisjoner

Personopplysningslovens § 2 gir følgende førende definisjoner:

1) Personopplysning	- opplysninger og vurderinger som kan knyttes til enkeltperson
2) Behandling av personopplysninger	- enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksområder
3) Personregister	- registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen
4) Behandlingsansvarlig	- den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes
5) Datatbehandler	- den som behandler personopplysninger på vegne av den behandlingsansvarlige
6) Registrert	- den som en personopplysning kan knyttes til
7) Samtykke	- en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv
8) Sensitive personopplysninger	- Opplysninger om: a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling c) helseforhold d) seksuelle forhold e) medlemsskap i fagforeninger

Videre defineres følgende sentrale begreper i dette dokumentet:

Datakommunikasjon	– elektronisk kommunikasjon av data i et informasjonssystem. Datakommunikasjon der overføringsmedium er utenfor virksomhetens kontroll betegnes *ekstern datakommunikasjon.*

Demilitarisert sone (DMZ)	– en sone hvor brukere utenfor virksomheten kan gis tilgang, men som er skilt fra virksomhetens øvrige informasjonssystem ved hjelp av en sikkerhetsbarriere.
Eksternt nettverk	– datanettverk som benyttes av flere virksomheter.
Internt nettverk	– fellesbegrep for de ulike nettverk som finnes i en virksomhet til bruk for de ansatte.
Område	– del av virksomheten adskilt fra virksomheten for øvrig ved hjelp av fysiske innretninger og med adgangskontroll.
Sone	– de deler av informasjonssystemet som kan kommunisere ved hjelp av datakommunikasjon. Soner opprettes etter analyse av behovet for tilgang og datakommunikasjon mellom enkelte enheter i informasjonssystemet.
Teknisk sikkerhetsbarriere	– utstyr og program benyttet for tilgangskontroll mellom virksomhetens informasjonssystem og eksterne nettverk, eller mellom forskjellige soner internt i virksomhetens informasjonssystem.
Virksomhet	– Den behandlingsansvarliges virksomhet (eksempelvis kommune, fylkes kommune, bydel eller KS), eller annen virksomhet det samarbeides med.

2. Formål

Formålet er først og fremst å dekke Personopplysningsloven av 14.04.2000 og Personopplysningsforskriften av 23.08.2005 og Helseregisterloven av 18.05.2001 sine krav til behandling av personopplysninger.
Håndboken er bygget opp etter Datatilsynets "Veileder for informasjonsikkerhet for kommuner og fylker" av 15.02.2005, "Veileder for personvernombud" av januar 2006 samt. norm for informasjonssikkerhet av 02.06.2010. Nedenfor er det utdrag fra kapittel 20 i veilederen som beskriver kravene til dokumentasjon. I kursiv skrift er det beskrevet hvordan håndboken innfrir disse kravene.

Dokumentasjonskontroll

Dokumentasjon skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll. Formålet med dokumentasjonskontrollen er å sikre at alle dokumenter er resultat av en ansvarlig beslutning, at de er korrekt utformet og kjent av virksomhetens ansatte i den grad dette er nødvendig for å utføre pålagte oppgaver.
Utarbeidelse av dokumentasjon av dokumenter skal gjennomføres slik at:

• det fastlegges hvem som er ansvarlig for utforming av dokumentet, herunder ansvar og myndighet for godkjenning av endrede og nye dokumenter	*Beskrevet i kapittel tre i håndboken*
• formålet med dokumentet beskrives	*Beskrevet i dette kapittel*
• dokumentet gis en entydig identifikasjon (navn, versjon og dato)	*Fremgår av forside, og på topp-teksten på alle skjema*
• det eksisterer retningslinjer for dokumentutforming	*Beskrevet i dette kapittel*
• det gis beskrivelse av media (elektronisk, papir) og arkivering av dokumentet	*Beskrives av kommunen*
• det fremgår hvem dokumentet skal distribueres til	*Fremkommer under målgruppe i hvert kapittel*
• dette settes i verk for nye og endrede dokumenter.	

Styrende dokumenter

Følgende styrende dokumenter skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll:

• sikkerhetsmål	*Beskrevet i kap. 4*
• sikkerhetsstrategi	*Beskrevet i kap. 5*
• oversikt og klassifisering av personopplysinger	*Beskrevet i kap. 6*
• informasjon om ansvars- og myndighetsforhold, organisasjonskart	*Beskrevet i kap. 3*
• konfigurasjonskart med informasjon om teknisk sikkerhetsløsning	*Beskrevet i kap. 10*
• informasjon om partnere og leverandører	*Beskrevet i kap. 12*
• Stillingsbeskrivelser skal utarbeides og distribueres i henhold til denne rutinen i den grad det er nødvendig for å få en tilfredsstillende informasjonssikkerhet. Strategiske	*Beskrevet i kap. 3*

planer bør • også inngå som styrende dokumenter.	

Prosedyrer

Prosedyrer av betydning for informasjonssikkerheten skal utarbeides og distribueres i henhold til rutine for dokumentasjonskontroll. Dette gjelder spesielt rutiner for:

• risikovurdering	*Beskrevet i kap.7*	˜ . sikkerhetsrevisjon	*Beskrevet i kap.8*
• ledelsens gjennomgang	*Beskrevet i kap.9*	˜ . konfigurasjonsendring	*Beskrevet i kap.10*
• beredskapsplaner	*Ikke beskrevet*	˜ . avviksbehandling	*Beskrevet i kap.11*
• adgangskontroll	*Beskrevet i kap.14*	˜ . tilgangskontroll	*Beskrevet i kap.13*
• datakommunikasjon	*Beskrevet i kap.*	˜ . dokumentsikkerhet	*Beskrevet i kap.17*

Registreringer

Resultater fra arbeidet med informasjonssystemet skal registreres i den utstrekning det er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet. Følgende registreringer skal lagres i 5 år:

- resultater fra ledelsens gjennomgang, risikovurderinger, sikkerhetsrevisjoner
- og avviksbehandling
- oversikt over områder og utstyr med adgangskontroll
- oversikt over soner, data og program med tilgangskontroll
- autorisering av brukere
- avtaler med partnere, databehandlere og leverandører
- tidligere utgaver av godkjente tekniske og administrative prosedyrer.

Hendelsesregistrering (aktivitetslogg) omfatter områdene adgang, tilgang og datakommunikasjon samt forsøk på uautorisert bruk. Disse skal lagres i 3 måneder.

Hensikten med registreringene er sporbarhet på utført behandling. I sammenheng med informasjonssikkerhet vil slik registrering være et viktig hjelpemiddel for å avdekke og oppklare brudd på sikkerheten. Det skal etableres rutiner for gjennomgang av hendelsesregistre. Hendelser av betydning for informasjonssikkerheten skal behandles i henhold til prosedyre for avviksbehandling.
Bruk av logger begrenses til å benyttes i sikring og administrasjon av informasjonssystemet. Annen bruk av logger, eksempelvis oppfølging av de ansattes arbeidsinnsats, må ha et særskilt hjemmelsgrunnlag.

For internt informasjonssystem anbefales registrering av følgende i en aktivitetslogg:

- innlogging/utlogging
- aktivitet på brukerkonti utenfor arbeidstid

- store utskriftsjobber
- store filoverføringer
- filtilgang på andre enn egne kataloger
- endringer av brukerprivilegier og passord
- autorisert og forsøk på uautorisert bruk (lagres i minimum 2 år)
- omstart
- forsøk på å endre registreringer eller det som skal registreres.

For tekniske sikkerhetsløsninger som f.eks. brannmur anbefales registrering av følgende:
eksterne anrop til nettverksadresser i virksomhetens informasjonssystemer
- adresser i det eksterne datanettet som det kommuniseres med
- forsøk på å oppheve sperrer eller begrensninger som håndheves av brannmurendring av sikkerhetskonfigurering av brannmur
- omstart
- forsøk på å endre registreringer eller det som skal registreres

Når det gjelder elektroniske hendelser bør følgende parameter registreres i hendelsesregisteret:
- brukernavn
- tidspunkt
- terminal
- type hendelse
- resultat (vellykket, ikke vellykket).

Det skal utarbeides rutine for gjennomgang av hendelsesregistre som omfatter:
- hvem som skal ha ansvar for å gjennomgå registreringene
- hvor hyppig registreringene skal gjennomgås
- beskrivelse av "unormale" aktivitetsmønstre som bør undersøkes
- hvordan etterkontroll av "unormale" aktivitetsmønstre bør foretas
- hvordan eventuelle sikkerhetsbrudd eller mistanke om slikt skal følges opp
- hvem som har ansvar for sletting av registreringer ved lagringstidens utløp.

3. Ansvars- og myndighetsforhold, organisasjonskart

POL § 13 Informasjonssikkerhet*- Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.*
For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene

Bestemmelsen understreker at det er den behandlingsansvarlige, ved virksomhetens daglige ledelse, som skal sørge for tilfredsstillende informasjonssikkerhet, jf. personopplysningsloven § 13 samt personopplysningsforskriften kapittel 2, og dermed har ansvar for at bestemmelsene i dette kapittelet følges.

Dette ansvaret omfatter også at det årlig avsettes tilstrekkelige resurser, både personalmessige og økonomiske, slik at tilfredsstillende informasjonssikkerhet opprettholdes.

Organisering

POF § 2-7 Organisering *(utdrag) Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.*

Arbeidet med informasjonsbehandlingen skal organiseres slik at tilfredsstillende sikkerhet oppnås.

Dokumentreferanse:
Viser til kommunens Internkontrolldokument.
F:\HMS\Ferdig Lokal KS-Plan - Integreringsavdelingen\Overordnet IK dokument

Ansvar for IS (Informasjons Sikkerheten)

Ansvaret for informasjonssikkerheten i Hattfjelldal kommune er fordelt på seks nivåer:

1. Rådmannen

Rådmannen har det overordnete ansvar for at informasjonssikkerheten i kommunen ligger på et forsvarlig nivå. Dette kommer til uttrykk i kommunens sikkerhetspolicy.

2. Overordnet operativt ansvar for informasjonssikkerheten (sikkerhetsansvarlig sammen med personvernombud)

- har ansvar av koordinerende og samordnende art:

- foreslå nye handlingsplaner
- utarbeide og implementere sikkerhetshåndbok og tilstrekkelig med kontrollrutiner
- planlegge IS arbeidet
- etablere og vedlikeholde sikkerhetsnivået, herunder ajourhold av sikkerhetshåndboken, etc.
- løpende overvåking av avtalte IS handlinger slik at det vedtatte sikkerhetsnivået opprettholdes
- presisere og fordele IS ansvaret på vegne av den øverste ledelsen
- foreta stikkprøver for å kontrollere at vedtatte instrukser og retningslinjer etterleves
- utarbeide og oppdatere årlig statistisk oversikt over sikkerhetsbrudd samt forsøk på dette
- sende endringsmeldinger til personvernombudet
- utforme opplærings- og motivasjonsprogram for ivaretagelse av IS
- delta i faglige forum og/eller samarbeide med andre virksomheter for å opprettholde kunnskapsnivå om IS og nye trusler/farer.

Skjema 3.3 Sikkerhetsinstruks sikkerhetsansvarlig

3. Overordnet operativt ansvar for drift av informasjonssystemet (IKT-ansvarlig).

IKT-avdelingen har ansvaret for informasjonssikkerheten i forbindelse med:

- kommunikasjon, nettverk, brannmurer, servere, PCer og annet relevant utstyr
- i et samarbeide med autorisasjonsansvarlig gjennomføre tilgangskontroll
- kvalitet på maskinutstyr og programvare
- etablere og vedlikeholde konfigurasjonskontroll
- drift og produksjon
- avbruddsplaner (katastrofeplaner) for IT-funksjonen.
- generell daglig oppfølging og kontroll av logger og rapporter

4. Avdelingssjef/enhetsleder

Det daglige ansvar for informasjonssikkerheten ligger hos enhetslederne for de ulike kommunale enhetene. Ledelsen skal innenfor sitt ansvarsområde sørge for at forvaltning og bearbeiding av informasjon skjer på en forsvarlig måte, og innenfor rammen av gjeldende lover og forskrifter, instrukser og retningslinjer.

Dette innebærer:

- å ha nødvendige rutiner som sikrer tilgang, integritet og konfidensialitet i behandling av personopplysningene
- å ha oversikt over hvilke personopplysninger som blir behandla,
- ha oversikt over hvilke register en har,
- klassifisere registrene
- fastsette akseptabel risiko på de viktigste områdene
- bidra til årlig risikovurdering med tilhørende handlingsplan
- avvikshåndtering i samsvar med vanlig praksis i kommunen
- sikre at forholdet til partnere og leverandører (databehandlere utenfra, konsulenter, håndverkere, renholdere, vikarbyrå) er i samsvar med kravene i personopplysningsloven.
- sikre at overføring av materiale som inneholder sensitive personopplysninger skjer i samsvar med gjeldende retningslinjer.
- gi og tilbakekalle autorisasjon til elektroniske hjelpemiddel og lokaler.

Skjema 3.4 Sikkerhetsinstruks ledere

5. IKT-/informasjonssikkerhetsgruppen

IKT-avdelingen og informasjonssikkerhetsgruppen er kommunen sitt rådgivende organ i IKT og sikkerhetsspørmål -spørsmål ovenfor rådmannen. IKT og informasjonssikkerhetsgruppen har ansvaret for overordnete oppgaver som: måldefinisjoner, måloppnåelse/resultat, planarbeid – utdanning/opplæring, innkjøp, styring og driftspolitikk.

I sikkerhetssammenheng vil typiske oppgaver være:

- gjennomgang og godkjenning av prosedyrer og retningslinjer for IS
- overvåkning av vesentlige endringer i trusselbildet
- gjennomgang og overvåkning av sikkerhetshendelser
- godkjenning av større initiativ for å styrke IS (eks. handlingsplaner)
- delta på møter sammen med personvernombudet

6. Systemansvar

For hvert IT system skal det utpekes en systemeier. Systemeier er ansvarlig for:

- ha ansvar for nye versjoner som skal installeres
- ha kontakt med leverandør av IT-systemet vedrørende systemets funksjonalitet (nye ønsker, nye krav, feilrapportering o.l.)
- gjennomføre tildeling til aktuelle applikasjon

- ha kontakt med leverandør av IT-systemet vedrørende bruker-, system-, produksjons- og driftsdokumentasjon, slik at denne er på plass og fortløpende ajourholdt

7. Medarbeidere

IS er hver enkelt medarbeiders ansvar, da alle er avhengig av at kommunen fungerer effektivt og sikkert for å kunne nå sine mål. Et effektivt IS arbeide bygger på alle medarbeideres lojale holdning, medvirkning og initiativ. Alle medarbeidere skal:

- forstå betydningen av IS i forbindelse med eget arbeid
- praktisere og etterleve vedtatte IS tiltak, ta opp svakheter og foreslå forbedringer gjennom avviksrapportering.
- være ansvarlig for kvaliteten av det arbeid de utfører
- sette seg inn i Sikkerhetsinstruksen
- overholde taushetspliktregler og sikkerhetsbestemmelser

4. Sikkerhetspolicy

Kommunens sikkerhetsmål er beskrevet i eget dokument:
''SIKKERHETSMÅL OG STRATEGI" for HATTFJELLDAL KOMMUNE.

Utfyllende innhold til sikkerhetsmål finnes i linken nedenfor:
Sikkerhetsmål og strategi v.1
Sikkerhetsmål og strategi v.2.

5. Sikkerhetsstrategi

Kommunens strategi er beskrevet i eget dokument:
''SIKKERHETSMÅL OG STRATEGI" for HATTFJELLDAL KOMMUNE.

Utfyllende innhold til sikkerhetsmål finnes i linken nedenfor:
Sikkerhetsmål og strategi v.1
Sikkerhetsmål og strategi v.2.

6. Oversikt og klassifisering av personopplysninger

6.1 Loven

POL § 13 Informasjonssikkerhet-
Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene.

Oversiktskartleggingen er ikke omtalt i POF

6.2 Formål

Den behandlingsansvarlige skal utarbeide og holde oppdatert oversikt over de personopplysninger som behandles. Oppdateringen skal også omfatte endringer i de lagrede dataene som inneholder personopplysninger.

Oversikten danner grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og –strategi. Dessuten benyttes den som underlag ved risikoanalyser.

6.3 Omfang

Oversikten skal omfatte alle typer behandlinger hvor det enten finnes personopplysninger eller sensitive personopplysninger, uansett om de befinner seg i elektronisk eller manuell form (mapper, permer, cardex o.l.).

Dette omfatter også alle input- og output- data til elektroniske systemer. Som en del av kartleggingen må en også kartlegge plassering av skjermer og skrivere i forhold til innsyn av uvedkommende.

6.4 Målgruppe

Dette omfatter alle avdelinger hvor personopplysninger behandles.

6.5 Ansvar og deltagelse

Enhetsleder har et særlig ansvar for nødvendige rutiner som sikrer tilgang, integritet og konfidensialitet i behandling av personopplysningene
å ha oversikt over hvilke personopplysninger som blir behandlet i sin avdeling,
ha oversikt over hvilke register en har i avdelinga,
klassifisere registrene
sikre at formålet med behandlingen er samsvarende med den lovhjemmel som danner grunnlaget for behandlingen

Avdelingsleder er også ansvarlig for å sende melding til personvernombudet når det skjer endringer i behandlingene.

6.51 kontrollrutiner

Foruten enhetsleder skal sikkerhetsansvarlig sammen med personvernombudet oppbevare alle eksisterende behandlinger. Sikkerhetsansvarlig skal gjennom revisjonen årlig sjekke om det er gjort endringer, opphør eller tillagt nye behandlinger i den enkelte enhet. Personvernombudet tester også dette ved periodisk kontroll.

6.6 Rutinebeskrivelse

Oversikten over personopplysninger som behandles skal gi kortfattet informasjon om:

Prosess 1

hvilke opplysninger som lagres og formålet med behandlingen, jf. POL § 11
klassifikasjon av hvorvidt personopplysningene er sensitive eller ikke
melde- eller konsesjonspliktige
teknologiske sikkerhetstiltak med angivelse av sone eller nettverk
registerets omfang

Prosess 2

hvor opplysningene lagres og om de overføres via eksterne media
hjemmelsgrunnlag for å lagre informasjonen med bruk av IT, jf. POL § 11
sikring av konfidensialitet (inkl. kryptering, sletting); POF 2.11
sikring av tilgjengelighet (inkl. back up og alternativ drift); POF 2.12

integritet (inkl. ødeleggende program), POF 2.13

6.7 Fremgangsmåte

Sikkerhetsansvarlig tar seg av prosess 1 på følgende måte:
Fremskaffer nødvendig oversikt over elektroniske behandlinger fra IT-avdelingen.

Dernest sammen med avdelingslederne skaffe seg oversikt over alle manuelle- behandlinger og -registre. Det skal også tydelig fremgå om hvorvidt dokumenter eller registre inneholder sensitive opplysninger.

Under prosess 2 er det avdelingsleders ansvar å registrere disse opplysningene og treffe nødvendige tiltak for å sikrer tilgang, integritet og konfidensialitet i behandling av personopplysningene.

Når dette arbeidet er utført skal det utfylles meldeskjema for alle registrene som er meldepliktige og oversendes personvernombudet. Meldingen fornyes hvert 3. år.

6.8 Referanse

Henviser til

prosess 1: SKJEMA 6.2 Program
prosess 2: SKJEMA 6.1_Personopplysninger Oversikt personopplysninger som behandles
SKJEMA 6.3 Håndtering av personopplysninger
Meldeskjema for personvernombud
Innmelding i arkivplan.no

7. Risikovurderinger

7.1 Loven

POF § 2-4 Risikovurderinger*- Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.*

Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og § 2-2
Resultatet av risikovurderingen skal dokumenteres.

7.2 Formål

Kommunen skal utføre risikovurdering med formål å få en oversikt over hvilken risiko virksomheten er utsatt for med eksisterende løsning. Det er viktig å få frem hvilke trusler som er mest sannsynlige å kunne inntre, og derigjennom hvor effektive sikkerhetstiltakene er, samt hvilken skade truslene kan påføre virksomheten og den enkelte.

Formålet med risikovurdering er også å undersøke hvorvidt den risiko som avdekkes er innenfor de akseptkriterier virksomheten har fastlagt.

7.3 Omfang

Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten endringer. Grundighet/omfang av risikovurderingen bestemmes ut fra den enkelte situasjon som skal vurderes.

Eksempler på forhold som kan kreve ny risikovurdering og godkjenning fra kommunens ledelse:

- ved iverksettelse av behandling av helse- og personopplysninger
- Endring i klassifikasjon av opplysningene
- Endringer i organisasjon
- Tekniske og bygningsmessige endringer
- Endringer i konfigurasjon
- Ekstern overføring av nye typer opplysninger
- Nye partnere eller leverandører
- Hjemmekontor og mobile enheter

7.4 Målgruppe

Ledelse, seksjonsledere og IT-ansvarlig

7.5 Ansvar og deltagelse

Risikovurderinger danner grunnlag for iverksetting av nødvendige sikkerhetstiltak, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten

Virksomhetens seksjonsledelse har ansvar for iverksetting av risikovurdering. Resultat fra analysen rapporteres "tjenestevei" som skal treffe avgjørelser over eventuelle tiltak. Ledelsen skal også fastsette nivået for akseptabel risiko.

7.51 Kontrollrutine

Under revisjon skal sikkerhetsansvarlig til en hver tid vurdere om risikovurderinger skal gjennomføres.

7.6 Rutinebeskrivelse

"Light"-utgaven - den enkleste formen for risikovurdering er vurderingen som utføres gjennom klassifikasjon av personopplysningen i form av å vurdere registrene i forhold til tilgjengelighet, konfidensialitet og integritet. Nedenfor er beskrevet en mere omfattende vurdering.

En mer inngående risikovurdering foretas dersom det foretas gjennomgående endringer slik som nevnt under 7.3 eller når ledelsen og sikkerhetsansvarlig mottar avviksmeldinger som krever en mere grundig gjennomgang av konsekvensen av avviket.

En slik risikovurdering skal gi følgende resultat:

- oversikt over identifiserte trusler
- angivelse av sannsynlighet for at en uønsket trussel kan inntreffe
- angivelse av konsekvenser av en trusselen
- resultat fra vurderingene av sikkerhetstiltakenes effekt i forhold til risiko
- risikoenvurdering vurderes opp mot hva som betegnes som akseptabel risiko (se pkt.7.61)

Helseopplysninger

For helseopplysninger skal nivå for akseptabel risiko fastsettes før behandling av helse- og personopplysninger startes og før risikovurderinger gjennomføres.. Her skal "Normen" følges – se Faktaark 5 i referanse

7.61 Nivå for akseptabel risiko

Akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet for helse- og personopplysninger i kommunen

Følgende vil være en norm for vurdering av risiko. Uønskede hendelser som havner i område:
- Rødt skal det gjennomføres tiltak for
- Gult skal det vurderes om det skal gjennomføres tiltak for
- Grønt er ikke nødvendig å gjennomføre tiltak for

Tilgjengelighet

Stans i systemet	<= 10 min	30 min	4 tim	8 tim
Sannsynlig: 4 Sannsynlig 365/1				
3 Mulig 12/1				
2 Mindre sannsynlig 1/1			6	
1 Usannsynlig 1/5				
	1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
	Konsekvens			

Det aksepteres ikke stans i tilgang til pasientrettede systemer med mer enn 4 timers varighet enn 1 gang per år(S = 2 og K = 3 gir nivå for akseptabel risiko på 6)

Konfidensialitet

Uautorisert innsyn i helse- og personopplysninger (lesetilgang)	Ingen	Innsyn i enkelte helse- og person-opplysninger og lovbrudd for intern bruker	Innsyn i enkelte helse- og person-opplysninger, mulighet for endring og lovbrudd. Det gis tilgang til en ekstern bruker som ikke har tjenstlig behov for EPJ for en eller flere pas.	Fullt uautorisert innsyn eller mulighet for endring av alle- helse og person-opplysninger og lovbrudd
Sannsynlig: 4 Sannsynlig 365/1				
3 Mulig 12/1				
2 Mindre sannsynlig 1/1			6	
1 Usannsynlig 1/5				
	1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk

Det aksepteres ikke at uvedkommende får innsyn i helse- og personopplysninger mer enn en gang per år (S = 2 og K = 3 gir nivå for akseptabel risiko på 6)

Kvalitet

Journal		Er komplett uten fare for pasienters helse	Noen mangler uten fare for pasienters helse	Viktig informasjon mangler i journal og brudd på lov med fare for pasienters helse og liv	Kritisk informasjon mangler i journal og brudd på lov. Diagnose feilkodes der det benyttes kodeverk. Medikament, dosering, behandlingstiltak blir feilregistrert. Helse- og personopplysninger blir henført til feil person. Med fare for tap av liv.
Sannsynlig	4 Sannsynlig 365/1				
	3 Mulig 12/1				
	2 Mindre sannsynlig 1/1			6	
	1 Usannsynlig 1/5				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

Det aksepteres ikke at kritisk informasjon mangler, diagnoser kodes feil eller medikament, dosering eller behandlingstiltak blir feilregistrert eller at helse- og personopplysninger blir henført til feil person oftere enn en gang per år med fare for tap av helse og liv (S = 2 og K = 3 gir akseptabel risiko på 6)

Konfidensialitet

Brudd på personvern, dvs at helse- og personopplysninger blir offentliggjort		Intet brudd	Brudd for et lite antall pasienter internt	Brudd for et stort antall pasienter internt	Brudd for et lite antall pasienter eksternt
Sannsynlig	4 Sannsynlig 365/1				
	3 Mulig 12/1				
	2 Mindre sannsynlig 1/1		4		
	1 Usannsynlig 1/5				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

Det aksepteres ikke brudd på personvernet mer enn en gang per år for et lite antall pasienter(S = 2 og K = 2 gir nivå for akseptabel risiko på 4)

Integritet

Tap av helse- og personopplysninger		Ingen fare for pasienters helse	Moderat uten fare for pasienters helse	Alvorlig med fare for tap av helse og liv	Uopprettelig med fare for tap av liv
Sannsynlig	4 Sannsynlig 365/1				
	3 Mulig 12/1		6		
	2 Mindre sannsynlig 1/1				
	1 Usannsynlig 1/5				
		1 Ubetydelig	2 Moderat	3 Alvorlig	4 Kritisk
		Konsekvens			

Registrerte helse- og personopplysninger skal ikke gå tapt oftere enn en gang per måned uten fare for pasienters helse(S = 3 og K = 2 gir nivå for akseptabel risiko på 6)

7.7 Fremgangsmåte

”Light”-utgaven – seksjonsleder skal gå kritisk gjennom vurdering av om konfidensialitet, tilgjengelighet og integritet er tilstrekkelig ivaretatt i forhold til formålbeskrivelsen. Vedkommende skal også treffe nødvendig tiltak og fastsette akseptkriteriet for akseptabel risiko. Om nødvendig skal akseptkriteriets nivå diskuteres med sikkerhetsansvarlig og rådmann.

Sikkerhetsansvarlig skal skaffe seg oversikt over planlagte endringer som er beskrevet i 7.3. og vurdere hvilke trusler dette kan forårsake. Egen sjekkliste for risikoområder er utarbeidet. I tillegg skal sikkerhetsansvarlig vurdere om det er avdekket trusler rundt:

- avviksrapportering
- personvernombudets kontroll - som gjør det nødvendig med risikovurdering.

Om nødvendig skal sikkerhetsansvarlig søke faglig assistanse for å gjennomføre vurderingen. Resultatet av risikovurderingen legges frem for berørte ledelse slik at sikkerheten blir tilstrekkelig ivaretatt i de forandringsprosessene som planlegges.

Sikkerhetsansvarlig skal jevnlig gjennomgå avviksmeldingene for å vurdere om tiltakene er tilstrekkelig ivaretatt og om trusselen kan ha gyldighet utover den seksjon som har meddelt avviket. Dersom sistnevnte er tilfelle skal sikkerhetsansvarlig gjennomføre risikovurdering og legge resultatet av vurderingen frem for ledelsen. Personvernombudet skal også påpeke behovet for risikovurdering der vedkommende ser det nødvendig.

7.8 Referanse

For øvrig henvises til Datatilsynets egen: ”Risikovurdering av informasjonssystem med utgangspunkt i forskrift for personopplysningsloven”.

SKJEMA 7.1_Risikovurderinger (Se også kommunens ROS analyse)
FAKTAARK 5 – Akseptkriterier (Normen)

8. Sikkerhetsrevisjon

8.1 Loven

POF § 2-5 Sikkerhetsrevisjon *- Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6. Resultatet fra sikkerhetsrevisjon skal dokumenteres.*

8.2 Formål

Formålet med sikkerhetsrevisjon er å sikre at besluttet sikkerhetsmål, -strategi og organisering etterleves i hele virksomheten.

8.3 Omfang

Sikkerhetsrevisjon skal gjennomføres slik at alle deler av virksomheten kontrolleres innenfor et 12 måneders intervall. Sikkerhetsansvarlig og personvernombud skal periodisk kontrollere arbeidet med informasjonssystemet og informasjonssikkerheten.

8.4 Ansvar og deltagelse

Virksomhetens ledelse v/ rådmann har ansvar for iverksetting av sikkerhetsrevisjon. Sikkerhetsrevisjoner skal ledes av sikkerhetsansvarlig med støtte fra personvernombudet og enhetsleder. Gjennomføringen bør utføres slik at den som leder kontrollen ikke selv er ansvarlig for den del av virksomheten som kontrolleres. I denne sammenheng har personvernombudet en viktig rolle som kontrollør. Personvernombudets arbeide er regulert i egen kontrakt.

8.41 Kontrollrutine

Rådmannen skal kontrollere at sikkerhetsrevisjon blir gjennomført.

8.5 Rutinebeskrivelse

Ved gjennomføring av kontrollen skal bl.a. følgende elementer gjennomgås:

- utførelse av arbeidsoppgaver i tilknytting til informasjonssystemet (jf. HP)
- sikkerhetstiltak, herunder utprøving av tekniske sikkerhetsløsninger
- gjennomgang av avvik registrert siden forrige kontroll samt kontroll av gjengangere i avdelingen
- kontroll av tilgangstyringen
- plassering av ansvar og organisering av sikkerhetsarbeidet
- kvalitet på sikkerhetsmål og sikkerhetsstrategi
- overholdelse av prosedyrer for bruk av informasjonssystemer og helse- og personopplysninger
- resultat av opplæring
- forvaltning og bruk av helse- og personopplysninger
- tilgang til helse- og personopplysninger og tiltak mot uautorisert innsyn

- effekten av etablerte sikkerhetstiltak ivaretakelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører
- Elementer i sikkerhetskontrollen:
- kontrollplan
- varsling om kontroll
- utarbeidelse av sjekkliste
- rapportering

Resultat fra sikkerhetsrevisjon rapporteres til virksomhetens ledelse. Eventuelle avvik avdekket i sikkerhetsrevisjon, behandles i samsvar med virksomhetens avvikssystem

Resultat av sikkerhetsrevisjon danner grunnlag for eventuelle endringer i sikkerhetsmål, -strategi og organisering, og inngår i underlaget for ledelsens gjennomgang av informasjonssystemet og informasjonssikkerheten.

8.6 Fremgangsmåte

Personvernombudet sammen med sikkerhetsansvarlig legger planer for gjennomføring av sikkerhetskontrollen. Som grunnlag for dette arbeidet legges sjekklisten for internkontroll fra Datatilsynet og Normen til grunn.

Sikkerhetsansvarlig er ansvarlig for å følge opp kontrollpunktene som er beskrevet i prosedyrene.

Personvernombudet tar igjennom sine kommunebesøk stikkprøver i organisasjonen om det er samsvar mellom teori og praksis.

På bakgrunn av dette lages felles rapport som leveres kommunens ledelse v/rådmann.

8.7 Referanse

Dokumentreferanse:

SKJEMA 8_Sikkerhetsrevisjon	Sikkerhetsrevisjon – kontrollplan
Kontrakt	Kontrakt mellom personvernombud og kommunen
Kontrollspørsmål til ledere og medarbeidere	

9. Ledelsens gjennomgang.

9.1 Loven

POF § 2-3. ***Sikkerhetsledelse*** *- Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet 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.

9.2 Formål

Løpende saker gjennom året
Sikre at informasjonssikkerhetsperspektivet blir ivaretatt ved løpende behandling av saker som berører papirbaserte eller elektroniske informasjonssystemer.

Den årlige hovedgjennomgangen
Oppsummere status for informasjonssikkerhetsarbeidet i kommunen
sikre at mål, organisering og handlingsplan er i samsvar med gjeldende lover og forskrifter
foreta eventuelle revisjoner

9.3 OMFANG

Prosedyren gjelder representanter fra kommunens øverste ledelse, sikkerhetsansvarlig, personvernombud og IKT-ledelse.

9.4 Ansvar og deltagelse
Sikkerhetsansvarlig og ledelsen i kommunen har særlig ansvar for gjennomføring av prosedyren

9.41 Kontrollrutine

Rådmannen har ansvaret for at ledelsesgjennomgangen blir gjennomført.

9.5 Rutinebeskrivelse

Løpende saker gjennom året kan være
viktige saker som kommer fram gjennom avviksbehandling, saksbehandling eller planlegging
rapporter fra offentlige tilsyn som angår informasjonssikkerhet.
Alle saker som berører viktige prinsipp i papirbaserte og elektroniske informasjonssystem, skal vurderes i vurdere samsvar med lovgiving om informasjonssikkerhet

Ved årlig hovedgjennomgang skal følgende vurderes:

- resultat fra sikkerhetsrevisjoner
- resultat fra risikovurderinger
- resultater fra avviksbehandling. Virksomhetens ledelse skal regelmessig følge opp at tiltak på grunnlag av avvik fastlegges, planlegges og gjennomføres
- ansvarsforhold og organisering mht. sikkerhet
- formål med behandling av helse- og personopplysninger og oversikt over helse- og personopplysninger som behandles i virksomheten
- konfigurasjonskart over informasjonssystemene. sikkerhetsmål, nivå for akseptabel risiko og strategier for informasjonssikkerhet
- endringer i lover og forskrifter
- endringer i type register som foretaket skal behandle
- endringer i trusselbildet som kommer fram i gjennomførte risikovurderinger
- ny funksjonalitet eller utvidet bruk.
- organisatoriske endringer
- bygningsmessige endringer

9.6 Framgangsmåte

Sikkerhetsansvarlig sammen med personvernombudet og kommunen ledelse gjennomgår både periodisk- og årlig kontroll på punktene beskrevet under 9.5. Resultatet av denne gjennomgangen skal lede til:

for periodisk kontroll – ny handlingsplan
for årlig gjennomgang – evt. ny policy, ny strategi og handlingsplan.
Tiltaksplan dersom risikovurderinger avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko?

9.7 Dokumentasjon og arkivering:

I tillegg til arkivering i samsvar med vanlige prosedyrer, arkiveres referat og vedtak fra disse punktene.

9.8 Referanser:

Personopplysningsloven med forskrifter
Helseregisterloven
Helsepersonelloven
Journalforskriften

Dokumentreferanse:

SKJEMA 9_Rapportering Rapport fra ledelsens gjennomgang.

10. Konfigurasjon

10.1 Formål

Formålet med konfigurasjonskontrollen er å sikre at utstyr og program fungerer sammen som forutsatt, samt at virksomhetene til enhver tid har en oppdatert oversikt over informasjonssystemets konfigurasjon, bl.a. til bruk ved risikoanalyser, egenkontroll, ledelsens gjennomgang av informasjonssystemet og av informasjonssikkerheten mv.

Formålet er å sikre at konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi, og at informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført.

10.2 Omfang

Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås. Konfigurasjonskontrollen omfatter all programvare, servere, nettverksutstyr, eksterne tilkoblinger som kommunen disponerer. Det samme gjelder koblinger mot eksterne partnere. Kun utstyr eller program eiet / disponert av virksomheten skal inngå i konfigurasjonen. Dette gjelder også utstyr eller program benyttet på hjemmekontor.

10.3 Målgruppe

IKT-avdeling, tilsynspersonell fra Datatilsynet og deltagere i ledelsesgjennomgangen

10.4 Ansvar og deltagelse

IKT-avdelingen er ansvarlig for utforming og vedlikehold av konfigurasjonene. Foretakets eksterne IKT-partner kan også gi et viktig bidrag til utformingen av konfigurasjon og vedlikeholde endringer. Ved outsourcing eller kommunevertskap (databehandler) av driftstjenester på vegne av kommunen skal det finnes egne avtaler som regulerer dette. (ServiceLeverings Avtale – SLA)

Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk, og bare etter godkjenning fra virksomhetens ledelse.

10.41 Kontrollrutine

Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

10.5 Rutinebeskrivelse

KONFIGURASJONSKONTROLL

IT-sansvarlig skal utarbeide en tegning over den IT-tekniske løsningen.
Viktige forhold som må komme klart frem er beskrevet i SKJEMA 10.1A – Konfigurasjonskart

Videre skal utstyr eller programmer med betydning for informasjonssikkerheten, herunder tekniske sikkerhetsbarrierer, dokumenteres. Slik dokumentasjon skal minimum omfatte:

- navn eller modellbetegnelse, og serienummer eller versjonsnummer
- sikkerhetsfunksjoner med opplysninger om oppsett/innstilling av utstyr/program
- når utstyret ble tatt i bruk, eller når utstyret ble tatt ut av bruk
- opplysninger om vedlikehold, skade, funksjonsfeil, reparasjoner.

Forslag til innhold for beskrivelse av den tekniske løsningen er beskrevet i SKJEMA 10.1B – Konfigurasjonskart – samt kap. 18 i kommuneveilederen

Konfigurasjonsendringer

Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk, og bare etter godkjenning fra virksomhetens ledelse.

Formålet er å sikre at konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi, og at informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført.

Sentrale elementer ved endring av konfigurasjonen er:
- behovs- og kompatibilitetsanalyse
- risikovurdering som viser at nivå for akseptabel risiko oppfylles
- som sikrer at forventede funksjoner er ivaretatt
- implementering som sikrer mot uforutsette hendelser
- ny konfigurasjon er dokumentert

Endringer av informasjonssystemets konfigurasjon besluttes av virksomhetens ledelse eller den ledelsen bemyndiger

Arbeidet med selve gjennomføringen av endringen kan delegeres virksomhetens ITdriftsleder.

10.6 Framgangsmåte

10.7 Referanser

Dokumentreferanse:

SKJEMA 10.1A_Konfiguasjonskart	IT-infrastrukturskisse
SKJEMA 10.1B_Komponentliste	Dokumentasjon på utstyr eller program med betydning for kommunen sin informasjonssikkerhet.
Service Leverings Avtale	Ved outsourcing av driftstjenester

SKJEMA 10.1C Beskrivelse av informasjonssystemet

11. Avviksbehandling

11.1 Loven

POF § 2-6 avviksbehandling *- Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles. Resultatet fra avviksbehandling skal dokumenteres*

11.2 Formål

Formålet med avviksbehandling er å bringe avviket til opphør, gjenopprette normal tilstand, og hindre gjentagelse. Dersom det ikke er samsvar mellom fastlagte rutiner og hvordan informasjonssystemet faktisk benyttes, skal resultatet fra avviksbehandling benyttes som grunnlag ved gjennomgang og endring av de aktuelle rutiner

Dersom informasjonssystemet benyttes i strid med fastlagte rutiner, ved brudd på informasjonssikkerhet, samt mistanke om sikkerhetsbrudd, skal virksomheten iverksette avviksbehandling.

11.3 Omfang

Omfatter alle enheter og steder der personopplysninger behandles, også institusjoner hvor det forkommer outsourcing av tjenester.

11.4 Målgruppe

Enhetsledere, sikkerhetsansvarlig og rådmannen.

11.5 Ansvar og deltagelse

Enhetsleder er ansvarlig for at det etableres praksis for avvikshåntering. Rapporteringspliktig er alle medarbeidere som behandler personopplysninger.

11.51 Kontrollrutine

Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

11.6 Rutinebeskrivelse

Avviksbehandling består av:
avdekking av avviket
rapportering; normalt utføres dette av den medarbeider som oppdager avviket.
Avviket rapporteres til virksomhetens nærmeste overordnede og til sikkerhetsansvarlig.

Iverksetting av tiltak bl.a. med det formål å avgrense eventuelle følgeskader. Tiltakene kan utføres av den medarbeider som oppdager avviket, eventuelt av den medarbeider som betjener eller har ansvar for den berørte del av informasjonssystemet.
vurdering, etter noe tid, av hvorvidt det korrigerende tiltak fungerer etter sin hensikt. Vurderingen utføres av virksomhetens IT-driftssjef, eventuelt av sikkerhetsansvarlig ved gjennomføring av egenkontroll.

Eksempler på situasjoner som gjør det nødvendig å iverksette avviks-behandling:
- ved utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering
- når medarbeidere benytter informasjonssystemet uten autorisasjon
- ved feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet
- ved brudd på prosedyrer
- utskrift kommer på avveier
- bærbart utstyr blir stjålet
- papirjournal ligger åpent tilgjengelig
- bruker går fra arbeidsstasjon usikret
- bruker låner bort brukernavn og passord til andre
- bruker blir ikke fjernet ved fratredelse
- helse- og personopplysninger blir sendt i usikret e-post
- autorisert bruker får ikke tilgang
- urettmessig tilegnelse av taushetsbelagte opplysninger (snoking)
- ureglementert bruk av nødrettilgang

11.7 Framgangsmåte

Den som oppdager avviket fyller ut avvikskjema med informasjon om:
hva som skjedde
evnt. feilmeldinger som fremkommer fra programvare eller IT-systemet
påfører også årsaken til avviket dersom dette er kjent

Avviksskjemaet sendes så nærmeste overordnede som har ansvaret for korrigerende tiltak. Kopi av avviket og tiltaket sendes sikkerhetsansvarlig. Mere alvorlige avvik drøftes med sikkerhetsansvarlig.

For de tilfeller der avviksbehandlingen har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet meddeles resultatet fra avviksbehandlingen.

11.8 Referanser

Dokumentreferanse:

SKJEMA 11_Avviksrapportering	Rapportering av alle typer hendelser; feil, sikkerhetsbrudd o.l.

12. Partnere og leverandører

12.1 Loven

POF § 2-15. *Sikkerhet hos andre virksomheter - Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.*

Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven § 29 og §30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.

Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet.

Den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale.

Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet

12.2 Formål

Kontraktsregulering av forholdet til partnere og leverandører har som formål å avklare ansvarsdelingen mht. informasjonssikkerhet, samt å utstyre virksomheten med et styringsverktøy overfor partner og leverandør.

12.3 Omfang

Regulering omfatter ikke bare IT-området men samtlige fagområder der det utøves samarbeide. Eksempler på partnere eller leverandører hvor det er aktuelt å inngå kontrakt med sikkerhetsvilkår:

- databehandlere
- firma med konsulentoppdrag
- firma som utfører vedlikehold av utstyr eller program, eller som utfører arbeid i områder hvor utstyr eller program befinner seg
- renholdsfirma
- vikarbyrå
- handverkere

12.4 Målgruppe

Innkjøpsansvarlig i alle enhetene.

12.5 Ansvar og deltagelse

Innkjøpsansvarlig/innkjøpsavdeling har her et særskilt ansvar for å innarbeide nødvendige tekster i anbudsdokumenteter som skal ivareta informasjonssikkerheten og som skal komme til uttrykk i kontraktsgrunnlaget

Innkjøpsansvarlig/innkjøpsavdeling skal også være kjent med sikkerhetsarbeidet hos leverandører der det inngår i elektronisk samhandling.

12.51 Kontrollrutine

Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

12.6 Rutinebeskrivelse

Rutinen kan grupperes i mere langsiktige avtaleforhold som f.eks. rammeavtaler samt mere tilfeldige bruk av tjenester

Dersom virksomheten benytter partnere eller leverandører for behandling av personopplysninger, eller dersom slike gis adgang eller tilgang til utstyr eller program hvor slike opplysninger behandles, skal partner/leverandørforholdet reguleres i kontrakt. Kontrakten skal minst ha vilkår for informasjonssikkerhet som tilfredsstiller Veileder fra Datatilsynet: Databehandleravtaler etter personopplysningsloven og helseregisterloven av 26.05.2009 Fordeling av sikkerhetsoppgaver mellom virksomheten og leverandøren, skal i ”sum” gi informasjonssikkerhet som minst tilfredsstiller kravene i dette kapittelet.

Virksomheter som utfører behandlinger av personopplysninger på vegne av den behandlingsansvarlige betegnes databehandlere, og forholdet til disse reguleres gjennom en databehandleravtale (ServiceLeveringsAvtale – SLA – se referanse) hvor informasjonssikkerheten vil utgjøre en del. Dersom databehandler er databehandler for flere virksomheter, skal skille mellom dem risikovurderes?

Kommunen skal også fremskaffe oversikt over de leverandører som berører informasjonsikkerheten. Til dette benyttes skjema for ”Leverandøroversikt” - referanse

Av de sikkerhetskrav som fremgår av retningslinjene for informasjonssikkerhet skal det i kontrakten spesielt legges vekt på:

- om partneren eller leverandørens personell er informert om den taushetsplikt som gjelder og at slikt personell skal undertegne taushetserklæring
- at det etableres oversikt over hvilke av partnerens eller leverandørens personell som skal gis tilgang til informasjonssystemet eller adgang til områder eller utstyr - hvordan virksomhetens - kontroll av sikkerhet hos partner og leverandør skal utføres.

12.7 Fremgangsmåte

Dette innebærer at innkjøpsleder eller innkjøper skal forsikre seg om at informasjonssikkerheten hos partner/leverandør er tilfredsstillende. Dette kan oppnås ved at den kommunen meddeles resultatet fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandling som er relevant for forholdet til partner/leverandør.

Eksempel på vilkår som bør inngå i kontrakt mellom virksomheten og partner/leverandør:

Ansvar

Leverandøren er ansvarlig for sikkerhetsbrudd for eget personale og brudd som har oppstått gjennom tilkopling av leverandørens utstyr. Leverandøren kan ikke engasjere en tredjepart (underleverandør) til å utføre arbeidsoppgaver som følger av denne avtalen, uten at oppdragsgiver har godkjent dette og leverandøren har inngått kontrakt med tredjepart som har tilsvarende sikkerhetsbestemmelser.

Taushetsplikt

Leverandørens personale skal undertegne taushetserklæring. De som undertegner taushetserklæring skal gjøres kjent med hva dette innebærer. Leverandøren kan kun benytte de personer til oppdraget som oppdragsgiver på forhånd har godkjent og er informert om.
Taushetsplikten gjelder også etter at avtalen er opphørt, og etter at leverandørens personale har sluttet hos leverandøren.

Sikkerhetsløsning

Leverandøren skal til enhver tid ha en organisatorisk og teknisk sikkerhetsløsning som tilfredsstiller Datatilsynets retningslinjer. Dette skal kunne dokumenteres overfor oppdragsgiver og Datatilsynet.

Samarbeid

Leverandøren skal ved behov samarbeide med oppdragsgiver om de sikkerhetsbrudd som kan tilskrives leverandøren. Som ledd i virksomhetens årlige egenkontroll, bør det være et møte for å gjennomgå leverandørens organisatoriske og tekniske sikkerhetstiltak

12.8 Referanse

Dokumentreferanse:

SKJEMA 12.1A_Leverandøroversikt	Oversikt over leverandørgrupperinger fordelt på tre grupper
SKJEMA 12.1B_Taushet partnere	Taushetserklæring KOMMUNE for partnere og leverandører.
Veileder - MAL for SLA (Se egen mal hos Rådmann)	Veileder til utforming av SLA for databehandlere

13. Personellsikkerhet

13.1 Kompetansekrav

13.11 Loven

POF § 2-8, siste avsnitt *- Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.*

13.12 Formål

Alle medarbeidere som bruker, administrerer, vedlikeholder eller utvikler informasjonssystemene eller på annen måte påvirker informasjonssikkerheten, skal ha nødvendig kompetanse til å utføre pålagte oppgaver.

13.13 Omfang

Omfatter at personell som har nøkkeloppgaver i forhold til informasjonssikkerhet samt alle medarbeidere som behandler personopplysninger.

13.14 Målgruppe

Omfattet ledere, enhetsledere og personalkontor.

13.15 Ansvar og deltagelse

Det skal utarbeides rutiner som ivaretar at kompetanse skal vedlikeholdes og utvikles. Ansvaret for dette tillegges sikkerhetsansvarlig og personalavdeling i et nødvendig samarbeid.

13.151 Kontrollrutine

Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

13.16 Rutinebeskrivelse

Sentrale elementer i en slik rutine består av:

- Oversikt over den enkelte medarbeiders kompetanse.
- Oversikt over kompetansekrav for de ulike oppgaver og funksjoner.
- Årlige planer for kompetanseutvikling.

De årlige medarbeidersamtalene er et godt utgangspunkt for å drøfte status og videreutvikling av kompetanse hos medarbeidere.

13.17 Fremgangsmåte

For nøkkelpersonellet gjennomføres kurs spesielt når enhetslederne er samlet. Ansvarlig for gjennomføringen er sikkerhetsansvarlig m/ ev. assistanse fra personvernombud. Videre vil sikkerhetsansvarlig gjennomføre opplæring i forbindelse med datafangst (prosess2 under 5.6)

For medarbeiderne kreves det i forbindelse med autorisasjonsrutinen at en har lest og gjort seg kjent med Sikkerhetsinstruksen. Enhetslederen skal sørge for at Sikkerhetsinstruksen følges og bevisstgjøre medarbeiderne om Sikkerhetsinstruksens innhold.

13.18 Referanse
Kapittel 3 i håndboken – for nøkkelpersonell
Sikkerhetsinstruks v5 – for medarbeidere og nøkkelpersonell

13.2 Autorisasjon og tildeling samt taushetsplikt

13.21 Loven
POF § 2-8, første og siste ledd *- Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.*
Autorisert bruk av informasjonssystemet skal registreres

POF § 2-9, Taushetsplikt *- Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.*

13.22 Formål
Formålet med autorisasjonsrutinen er å sikre at de som får adgang til områder og utstyr og tilgang til soner, data og program, til enhver tid har den autorisasjon som er nødvendig i forhold til tjenstlige behov.

Formålet er også å hindre gjennom taushetspliktreglene at ikke sensitiv informasjon kommer i hendene på uvedkommende

13.23 Omfang
Rutine for autorisasjonstildeling skal omfatte:

- autorisasjon av nytilsatte, vikarer og partnere med henhold til tjenstlige behov
- behov for endringer ved forandring av oppgaver, herunder sletting av autorisasjon når tjenstlige behov ikke lenger er tilstede, for eksempel når en medarbeider slutter i virksomheten eller går til annen stilling
- kontroll med at tildelte autorisasjoner fungerer etter forutsetningene.
- følge opp uregelmessigheter som f.eks. bruk av feil passord
- undertegning av taushetsløfte

13.24 Målgruppe
Rettet mot enhetsleder, fagansvarlig for programmer og IT-avdeling.

13.25 Ansvar og deltagelse
Enhetsleder eller delegert har ansvar for gjennomføring av autorisasjon på den enkelte enhet, herunder undertegning av taushetsløfte. Enhetsleder har ansvaret for å

dokumentere hvem som er gitt delegert autorisasjonsansvar til en hver tid. Enhetsleder har også ansvaret for å trekke tilbake autorisasjoner når medarbeidere slutter, går ut i permisjon eller går over i ny stilling.
Enhetsleder har ansvar for at rutinene er oppdatert og egnet for de områder eller rolle som rutinene skal betjene. Sikkerhetsansvarlig sammen med IKT-avdelingen skal utarbeide instruks for bruk av passord og tildeling av brukerindent.
IT-avdelingen og fagansvarlig for programvare har ansvar for gjennomføring av tildeling av de autorisasjoner som avdelingene bebuder.
Teknisk avdeling er ansvarlig for tildeling til de fysiske rom.

13.251 Kontrollrutine
Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

13.26 Fremgangsmåte
Den enkelte enhetsleder setter opp hvilken autorisasjon vedkommende skal ha og bestiller autorisasjonen hos IT-avdeling i god tid før vedkommende begynner

Første dag vedkommende er på jobb skal enhetsleder sørge for at taushetserklæring blir underskrevet. I tillegg skal standard bestillingsskjema for autorisasjon underskrives av både enhetsleder og eieren av ID'en og bruker skal underskrive egenerklæringskjemaet.

Autorisasjons-, taushets- og egenerklæringsskjema sendes personalkontoret for registrering. Personalkontoret kontrollerer taushets- og egenerklæringsskjemaet og oppbevarer disse. Autorisasjonsskjemaet sendes IT-avdelingen med påtegning om alt er ok.

Ved endring av en brukers organisasjon, jobbfunksjon eller rolle skal enhetsleder sammen med IT-avdelingen gjennomgå autorisasjon for vedkommende.

Ved endring til ny enhet skal ny enhetsleder kontakte IT-avdeling for eventuell endring av autorisasjon.

Alle nyinnmeldinger eller slettinger skal skje skriftlig via personalkontoret
Endringer av en bruker/autorisasjon skal skje skriftlig til IT-Avdelingen.

Ved behov for autorisering av servicepersonell gis autorisasjon i hvert enkelt tilfelle av innkjøpsansvarlig. Autorisasjon slettes umiddelbart etter oppdragets utførelse. Loggføres.

En gang pr. år skal enhetsleder gjennomgå autorisasjonene for den enkelte ansatte for kontroll. Liste over ansatte med den enkeltes autorisasjon stilles til disposisjon fra IKT-avdelingen.

13.27 Referanse
Dokumentreferanse:

Skjema 13.3B_Autorisasjon i Hattfjelldal kommune for fast ansatte og vikarer	
SKJEMA 13.2A_Taushet ansatte	Taushetserklæring for fast ansatte og vikarer
SKJEMA 13.3B Autorissjonsansvar	Autorisasjonsansvarlige i Hattfjelldal kommune.

Egenerklæring

14. Fysisk sikkerhet

14.1 Loven

POF § 2-10 Fysisk sikring *- Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her. Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten.*

Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.

14.2 Formål

- er å sikre at uvedkommende ikke får tilgang personopplysninger eller at de ikke er tilgjengelig når liv og helse står på spill.

14.3 Omfang

Behandlingsansvarlig skal sørge for at egne lokaler og utstyr er forsvarlig sikret, med spesiell vekt på de rom hvor det er plassert utstyr benyttet for behandling av personopplysninger, eller for sikring av slike (eksempelvis tjenermaskin, kommunikasjons-og nettverksenheter).

Adgang til lokaler og utstyr hvor personopplysninger behandles skal kontrolleres. Det gjelder spesielle sikringstiltak der hvor det behandles sensitive personopplysninger eller der man har informasjon om sikring av slike opplysninger.

Virksomheten må vurdere behovet for å innføre fysisk områdeinndeling av lokaler, slik at det er entydig hvilke områder som trenger spesiell beskyttelse. Denne sikringen kan gjennomføres ved bruk av adgangskontroll til lokaler eller bruk av spesielle sikringsmekanismer knyttet til bruk av selve utstyret.

Den fysiske sikringen av behandling av personopplysninger er en vesentlig del av det totale sikkerhetskonseptet. Trusler som kan utløses ved for dårlig fysisk sikring kan bl.a. være:
- at uvedkommende får tilgang til utstyr hvor personopplysninger behandles
- tyveri av arkiv, PC-er eller sikkerhetskopier på dagtid eller ved innbrudd utenom arbeidstiden
- sabotasje eller hærverk mot vitale deler av IT-systemet.

14.4 Målgruppe

Rettet mot ledelse, enhetsledelse, skkerhetsansvarlig og IT-avdeling.

14.5 Ansvar og deltagelse

14.51 Kontrollrutine
Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

14.6 Rutinebeskrivelse
Adgang til område
Ved bruk av områdesikring med adgangskontroll der sensitive personopplysninger behandles, skal det kontrolleres at kun autorisert personell har selvstendig adgang til disse. Dette innebærer følgende:

- områder der sensitive personopplysninger behandles skal være kontrollert av
- adgangskontrollsystem
- før nøkkelansvarlig tildeler den enkelte nøkler og koder for adgang, skal
- skriftlig autorisasjon mottas
- tildelte adgangsrettigheter skal begrenses til det som er nødvendig ut fra
- tjenstlig behov, og skal alltid fjernes når arbeidsforholdet opphører
- besøkende skal alltid følges av medarbeider som er autorisert for adgang til
- området, og skal aldri etterlates alene i slike områder.

Adgang til utstyr
Ved bruk av mekanismer for sikring av adgang til utstyr for behandling av sensitive personopplysninger, skal mulig bruk av utstyret begrenses til de som har tjenstlig behov for dette. Det utstyret som benyttes ved behandling av sensitive personopplysninger (arbeidsstasjoner og skrivere, kopimaskiner, telefaks etc.) må innrettes slik at tilgangen begrenses til de som har tjenstlig behov. Dette gjennomføres ved bruk av betryggende rutiner og teknisk sikring for å hindre uautorisert bruk at utstyret, samt egnede tiltak mot innsyn.

Sikring av andre lokaler
Utstyr benyttet på hjemmekontor skal fysisk sikres ved bruk av normal bygningsmessig sikkerhet. Videre bør det innskjerpes at avlåsing og lukking av vinduer blir gjort når lokalene ikke er i bruk.

14.7 Fremgangsmåte

14.8 Referanse
Dokumentreferanse:
SKJEMA 14 Fysisk sikkerhet

VIKTIG:
Skjemaet inneholder opplysninger om hvor informasjon befinner seg i kommunen.

Dokumentets innhold er derfor av en slik karakter at kun spesielt autorisert personell bør ha tilgang til dette dokumentet. Dette må du avgjøre for din kommune.
Ideelt sett bør dokumentet lagres kryptert på disk, og i utskrifts form på et sikkert sted.

15. Hendelsesregistrering

15.1 Loven

Personopplysningsforskriften § 2-14, § 2-16 og § 7-11..

15.2 Formål

Formålet med hendelsesregistrering og oppfølging av hendelsesregistre er å:
· gi oversikt over autorisert bruk av helse- og personopplysninger i virksomheten
· sette virksomheten i stand til å avdekke uautorisert bruk, eller forsøk på uautorisert bruk, av helse- og personopplysninger
· forebygge, avdekke og forhindre gjentagelse av sikkerhetsbrudd i informasjonssystemene
· legge til rette for pasient/brukers rett til innsyn i hendelsesregistre, slik at vedkommende gis mulighet til å ivareta egne rettigheter
· legge til rette for ansattes rett til innsyn i opplysninger som er lagret om vedkommende i hendelsesregisteret

15.3 Omfang

Alle virksomheter i sektoren som behandler helse- og personopplysninger elektronisk, skal føre og kontrollere hendelsesregistre

15.4 Målgruppe

Rettet mot ledelse, enhetsledelse, medarbeidere, databehandle, leverandør, sikkerhetsansvarlig og IKT-avdeling.

15.5 Ansvar og deltagelse

Databehandlingsansvarlig har ansvaret for hendelsesregistrering, men de daglige oppgavene er normalt delegert til den som er ansvarlig for det enkelte informasjonssystem.

15.51 Kontrollrutine

Sikkerhetsansvarlig skal kontrollere at prosedyren blir fulgt.

15.6 Rutinebeskrivelse

Hendelsesregistrering skal etableres for

a) Tilgang til behandlingsrettede helseregistre og fagsystemer
- All tilgang til og autorisert bruk av behandlingsrettede helseregistre og fagsystemer
- Alle forsøk på uautorisert bruk av behandlingsrettede helseregistre og fagsystemer
- All bruk av nødrettstilgang med begrunnelse

b) Infrastruktur

- Sikkerhetsrelevante hendelser i sikkerhetsbarrierer (for eksempel brannmur og ruter) slik som:
  - Alle forsøk på ulovlig tilgang både internt og eksternt
  - Alle brudd på regler som forbyr trafikk
  - Alle brudd på regler som slipper inn lovlig trafikk fra eksterne tilknytninger
  - Alle forsøk på uautorisert bruk av nettverksoperativsystemer

Hendelsesregisteret skal som minimum inneholde

a) For autorisert bruk:
- Entydig identifikator for den autoriserte brukeren (Se Faktaark 47 - Autorisasjonsregister)
- Rollen den autoriserte brukeren har ved tilgangen
- Virksomhetstilhørighet for den autoriserte brukeren (vanligvis virksomhet eller databehandler)
- Organisatorisk tilhørighet til den som er autorisert (avdelingsnavn eller avdelingskode er normalt tilstrekkelig). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur
- Hvilken type opplysninger det er gitt tilgang til
- Grunnlaget for tilgangen (for eksempel helsehjelp, nødrettstilgang, administrativ bruk)
- Tidspunkt og varighet for tilgangen (dato og klokkeslett)
- Begrunnelse ved bruk av nødrettstilgang

Ved fjernaksess fra leverandør:

o initiert trafikk mot IP-adresse og portnummer
o hva som er utført (kommandoer, transaksjoner, osv). Om mulig skal angivelse av tid for utført kommando også hendelsesregistreres
o hvilke data/datafiler som er lastet ned til leverandør (datafiler) eller opp til virksomhet (programfiler og patcher)
o Navn og entydig identifikator for den/de hos leverandør som har benyttet den aktuelle fjernaksess

b) For forsøk på uautorisert bruk:
- Brukeridentiteten som ble benyttet
- Tidspunkt (dato og klokkeslett)
- IP-adresse eller annen identifikasjon av PC/arbeidsstasjon som ble benyttet (for eksempel MAC-adresse eller NAT-adresse)

15.7 Fremgangsmåte

Sikring og oppbevaring av hendelsesregister

a) Hendelsesregistrene skal sikres mot innsyn, endring og sletting av uautorisert personell
b) Hendelsesregistre skal oppbevares i minimum 2 år
6. Hendelsesregisteret som bevis
a) Hendelsesregister som skal benyttes som bevis bør speilkopieres til annet medium før

analyser gjennomføres
b) Speilkopieringen bør gjennomføres under tilsyn av 2 eller flere personer
c) Det bør opprettes en skriftlig protokoll for speilkopieringen som sier hva som er gjort. Protokollen skal signeres av de som var tilstede og oppbevares sammen med det registrerte
avviket

15.71. **Bruk av hendelsesregisteret**

a) Elektroniske hendelsesregistre skal enkelt kunne analyseres ved hjelp av analyseverktøy
med henblikk på å oppdage brudd på regelverket (se også helseregisterloven § 13a og helsepersonelloven § 21 a.)
b) For manuelt førte hendelsesregistre skal virksomheten etablere prosedyrer for tilfredsstillende analyse av registrene
c) Dersom brudd avdekkes skal personalmessige reaksjoner iverksettes
d) Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt
tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes
e) All bruk av nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som
et avvik for å påse at begrunnelse er relevant
f) Ved brudd på regler ved tilkobling til nett utenfor virksomheten skal kanalen stenges inntil
ny sikker løsning er etablert
g) Ved brudd på regler om logisk skille mellom Internett og nettverk der helse- og personopplysninger behandles skal regelbruddet behandles som avvik og personalmessige
konsekvenser vurderes
h) Ved brudd på regler om at sensitive personopplysninger ikke skal utleveres ved hjelp av epost
skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes

15.72. **Sletting av hendelsesregistre**

a) Dersom oppføringer i hendelsesregistre kan knyttes til enkeltpersoner, skal hendelsesregistrene slettes når de sikkerhetsmessige formål er oppfylt, men først etter 2 år

15.8 Referanse

Dokumentreferanse:

16. Systemteknisk sikkerhet

Dette er et kapittel som har interesse i hovedsak for det tekniske personellet i kommunen og er derfor ikke tatt inn i håndboken. Henviser her til kapittel 18 i Veiledningen.

17. Dokumentsikkerhet

POF § 2-16. Dokumentasjon *- Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.*

Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.

Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten

Begrepet dokumenter omfatter i denne sammenheng så vel papirutskrifter som datafiler på elektroniske lagringsmedia som disketter, magnetbånd, CD-plater, harddisker etc. Dokumenter som inneholder personopplysninger eller informasjon om sikring av slike opplysninger skal behandles slik at:

det ved intern og ekstern forsendelse av slike dokumenter:

- bare er personer som har tjenstlig behov for tilgang til opplysningene som mottar slike dokumenter
- er mulig å oppdage uautorisert utlevering eller forsøk på slik utlevering, eksempelvis ved emballering/forsegling av dokumentet. Dette gjelder også ved bruk av virksomhetens interne postsystem, hvor flere enn den autoriserte kan ha tilgang.

det ved oppbevaring av dokumenter med personopplysninger:

- tydelig fremgår av dokument at det inneholder personopplysninger
- det er ivaretatt fysisk sikring når det ikke er under tilsyn av autorisert personell
- at utskrifter inneholdende personopplysninger ikke blir liggende på skriver eller lignende på utskriftssteder som kan være tilgjengelig for uautorisert personell.

Regler for sletting som beskrevet over omfatter også makulering av dokumenter som inneholder personopplysninger.

Vær i det hele årvåken for at utskrifter og dokumenter fra kommunen som ikke er vurdert som «åpen for alle», ikke havner i åpne søppelkontainere, på søppelfyllplass eller på annen måte kommer uvedkommende i hende (eks. gjenglemte dokumenter/rapporter på offentlige steder).

Bruk av telefaks

Det er ikke tillatt å sende sensitiv informasjon på telefaks.

Dokumentreferanse:

Arkivplan for kommune

18 Internkontroll og personvernombud

POF § 3-1 Systematiske tiltak for behandling av personopplysninger
Den behandlingsansvarlige skal etablere internkontroll i samsvar med personopplysningsloven § 14 De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av personopplysningsloven, med særlig vekt på bestemmelser gitt i medhold av personopplysningsloven § 13.
Internkontroll innebærer at den behandlingsansvarlige blant annet skal sørge for å ha kjennskap til gjeldende regler om behandling av personopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av de ovenstående rutiner, samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.
Den behandlingsansvarlige skal også ha rutiner for oppfyllelse av sine plikter og de registrertes rettigheter etter det til enhver tid gjeldende personvernregelverk, herunder ha rutiner for
a) innhenting og kontroll av de registrertes samtykke, jf. personopplysning-loven §§ 8, 9 og 11,
b) vurdering av formål med behandling av personopplysninger i samsvar med personopplysningsloven § 11 bokstav a,
c) vurdering av personopplysningenes kvalitet i forhold til det definerte formålet med behandling av opplysningene, jf. personopplysningsloven §§ 11 bokstav d og e, 27 og 28, samt oppfølging av eventuelle avvik,
d) oppfyllelse av begjæringer om innsyn og informasjon, jf. person - opplysningsloven §§ 16 til 24,
e) oppfyllelse av krav fra den registrerte om reservasjon mot visse former for behandling av personopplysninger, jf. personopplysningsloven §§ 25 og 26,
f) oppfyllelse av personopplysningslovens regler om melde- og konsesjons-plikt, jf. personopplysningsloven §§ 31 til 33.
Databehandlere som behandler personopplysninger på oppdrag fra behandlingsansvarlige, skal behandle opplysningene i samsvar med rutiner behandlingsansvarlige har oppstilt.

Dokumentreferanse:

Normens faktaark 6b sjekkliste
Sjekkliste internkontroll fra Datatilsynet 2009
Kommunens internkontroll POL/POF

Lovkrav
Hvilke krav i personopplysningsloven og forskriften påvirker kommunen?

Dokumentreferanse:

SKJEMA 18.1_Lov og forskrift Lovparagrafer i personopplysningsloven m/ forskrift som påvirker kommunen

Personvernombud

Kommunen har inngått avtale med personvertombud Alf Leinan. Ombudet skal bl.a. assistere kommunen med å implementere internkontroll og holde systemet ved like.

Personvernombudet skal gjennomfør de oppgaver som Datatilsynet fastsetter for at kommunene skal slippe fri fra meldeplikten.
For at Datatilsynet skal kunne unnta fra meldeplikten, må personvernombudet ha minst de følgende to oppgaver:
Sikre at den datadatabehandlingsansvarlige følger personopplysningsforskriften med forskrifter
Føre en oversikt over meldinger om virksomhetens behandling av personopplysninger

For behandlinger som er underlagt konsesjon, må konsesjonssøknad fremdeles sendes Datatilsynet jf. personopplysningsloven § 33 og helseregisterloven jf. §§ 5 flg.

Personvernombudet skal:

- påse at behandlinger meldes i samsvar med vilkår 2 ovenfor, vurdere om meldingene inneholder korrekte og tilstrekkelige opplysninger, og ved mistanke om feil eller mangler gjøre datadatabehandlingsansvarlige oppmerksom på dette,
- føre en systematisk og offentlig tilgjengelig fortegnelse over alle behandlinger som er innmeldt med opplysninger som nevnt i personopplysningslovens § 18, 1. ledd, jf. § 23,
- påse at datadatabehandlingsansvarlig har et system for internkontroll som tilfredstiller personopplysningslovens § 14, jf. personopplysningsforskriftens kap. 3,
- bistå registrerte med å ivareta deres rettigheter etter reglene om behandling av personopplysninger,
- påpeke brudd på regler om behandling av personopplysninger overfor datadatabehandlingsansvarlig,
- etter henvendelse fra Datatilsynet opplyse om eventuelle brudd på regler om behandling av personopplysninger og foreta undersøkelser i konkrete saker,
- holde seg orientert om utviklingen innen personvern og de problemer som knytter seg til behandling av personopplysninger, og
- gi råd og veiledning til datadatabehandlingsansvarlig om behandling av personopplysninger og reglene for dette.

I tillegg skal personvernombudet bistå datadatabehandlingsansvarlig under ledelsesgjennomgangen