RAKKESTAD KOMMUNE
KOMMUNESTYRET

MØTEINNKALLING

KOMMUNESTYRET
Møtedato/sted: 15.12.2011 Kommunestyesalen, Rådhuset kl: 18.00

SAKLISTE:

90/11
INFORMASJONSSIKKERHET I RAKKESTAD KOMMUNE - REVISJON AV SIKKERHETSHÅNDBOKEN

91/11
KOMMUNEPLAN FOR IDRETT OG FYSISK AKTIVITET 2012 - 2024 PRIORITERT HANDLINGSPROGRAM 2012 - 2015

92/11
FRIVILLIG VERN AV KOMMUNESKOG - ASKEVANN

Saksdokumentene følger vedlagt.

Saksdokumenter er utlagt på Servicekontoret og Biblioteket f.o.m 08.12.2011 og t.o.m møtedagen.

Sakskart med saksdokumenter ligger også på kommunens internettside
www.rakkestad.kommune.no

Kommunestyremøte overføres på Radio 5, frekvens 102,9.

De representanter som ikke kan møte p.g.a. lovlig forfall må omgående melde fra om dette til servicekontoret, tlf. 69225500. **Vararepresentanter møter kun etter nærmere innkalling herfra.**

Rakkestad, den 07.12.2011

Ellen Solbrække
Ordfører

RAKKESTAD KOMMUNE
KOMMUNESTYRET

Saksbehandler Kåre Kristiansen Arkiv nr. X57

Utvalg	Saknr	Møtedato
ARBEIDSMILJØUTVALGET	9/11	23.11.2011
FORMANNSKAPET	53/11	01.12.2011
KOMMUNESTYRET	90/11	15.12.2011

Utvalgssak 90/11 **Saknr 11/2248** **Løpenr 14414/11**

90-11 INFORMASJONSSIKKERHET I RAKKESTAD KOMMUNE - REVISJON AV SIKKERHETSHÅNDBOKEN

Rådmannens forslag til vedtak:

Kommunestyret vedtar "Sikkerhetshåndbok for informasjonssikkerheten" i Rakkestad kommune.

ARBEIDSMILJØUTVALGETs behandling:
Rådmannens forslag til vedtak enstemmig vedtatt

ARBEIDSMILJØUTVALGETs innstilling :
Kommunestyret vedtar "Sikkerhetshåndbok for informasjonssikkerheten" i Rakkestad kommune.

FORMANNSKAPETs behandling:

Utvalgsleders innstilling:
Ordfører innstiller i samsvar med rådmannens forslag til vedtak.

Ordføreres innstilling enstemmig vedtatt.

FORMANNSKAPETs innstilling til kommunestyret:
Kommunestyret vedtar "Sikkerhetshåndbok for informasjonssikkerheten" i Rakkestad kommune.

Saksopplysninger:

Vedlegg: Sikkerhetshåndbok med vedlegg (1-9)

Bakgrunn for saken:

Rakkestad kommune hadde sommeren 2011 en gjennomgang av sikkerhetsrutinene og etterfølgende oppdatering av sikkerhetshåndboken. Iflg Personopplysningsloven m/forskrifter skal slike revisjoner/kontroller gjennomføres jevnlig og skal omfatte alle enheter som behandler personopplysninger i kommunen.
Gjennomgangen og revisjonen er foretatt av Institutt for Datasikkerhet v/Torbjørn Skjølstad. Forrige revisjon var i 2008. Revisjonen viste at Rakkestad kommune har et høyt sikkerhetsnivå som i all hovedsak tilfredsstiller de viktigste sikkerhetskravene i lovverket.

Innholdet i sikkerhetshåndboken fastlegger Rakkestad kommunes krav til beskyttelse av informasjon som samles inn, lagres, bearbeides, overføres og formidles så vel manuelt som digitalt.

Innholdet i håndboken utgjør et felles rammeverk for det praktiske arbeid med informasjonssikkerhet i kommunen og skal benyttes:

- *for at de respektive tjenestesteder i kommunen skal kunne oppnå et nødvendig og riktig sikkerhetsnivå i sin daglige drift*
- *for å skape en felles sikkerhetskultur gjennom nødvendig opplæring og økt forståelse av behovet for informasjonssikkerhet*
- *for å etterleve kravene til informasjonssikkerhet i Personopplysningsloven og Helseregisterloven og annet relevant lovverk*
- *som grunnlag ved meldinger og som vedlegg til eventuelle senere konsesjonssøknader til Datatilsynet*

Kommunens ansvar for saken:

Kommunen er underlagt krav til informasjonssikkerhet i Personopplysningsloven og i Helseregisterloven m/forskrifter, og er i tillegg underlagt krav om profesjonsbestemt taushetsplikt bl.a. etter Forvaltningsloven og Helseopplysningsloven. All behandling av personopplysninger skal være i samsvar med disse krav og lover. Når det gjelder dokumentbehandling er også bestemmelser i Kommuneloven og Offentlighetsloven relevante.

Ved behandling av sensitive personopplysninger skal kravet til konfidensialitet ikke vike til fordel for kravet til tilgjengelighet.

Andre opplysninger:

Enhetsleder servicekontoret har vært utnevnt til sikkerhetskoordinator, denne oppgaven overtas nå av IT-enheten . Personvernombudrollen har en viktig rolle med kommunens utfordringer i å etterleve lovens krav og å bygge videre på de gode rutinene som allerede finnes for å møte stadig flere utfordringer forbundet med informasjonssikkerhet.

K o n s e k v e n s v u r d e r i n g e r :

Økonomi:
Sikkerhetshåndboken har ingen økonomiske konsekvenser for Rakkestad kommune ut over ordinær drift.

Arbeidsmiljøloven (for saker som skal behandles i AMU)
Den utarbeidede sikkerhetshåndboken er en del av et internkontrollsystem og skal behandles av AMU i.h.t. AML § 24 e.

Administrasjonens vurdering:
Informasjonssikkerhet er et lederansvar og Rakkestad kommune ønsker å fremstå som en seriøs aktør og en kommune som tar informasjonssikkerhet på alvor. Kommunen har de siste årene foretatt betydelig sikringstiltak, både elektronisk og fysisk.

Forslag til Sikkerhetshåndbok ble utarbeidet av Institutt for Datasikkerhet høsten 2011 og er etter dette bearbeidet internt i administrasjonen. Sikkerhetshåndboken er et verktøy og arbeidsredskap for å oppnå så god informasjonssikkerhet som mulig i kommunen. Det er den enkelte lederes ansvar å informere, og å sørge for at de ansatte har god nok kjennskap til å etterleve de råd og pålegg som følger av håndboken, og at beskrevne, nødvendige tiltak blir iverksatt og fulgt opp. Kommunens Sikkerhetskoordinator vil være viktige støttespillere i dette arbeidet.

Formålet med tiltakene i sikkerhetshåndboken er å formalisere en sikkerhet for at Rakkestad kommune behandler personopplysninger i tråd med lovverket og at innbyggerne i Rakkestad skal ha trygghet for at informasjon som blir gitt kommunen ikke kommer på avveie.

Hvorfor informasjonssikkerhet i Rakkestad kommune
Truslene mot informasjonssikkerheten kan ha sitt opphav internt i kommunen (medarbeidere/utstyr/rutiner) eller skyldes eksterne faktorer. De eksterne truslene vil øke som følge av økt bruk av nettverkstjenester, men de interne truslene bør fortsatt vies størst oppmerksomhet fordi manglende sikkerhetsforståelse internt kan utgjøre en større trussel enn omgivelsene.

Konsekvenser ved dårlig eller utilfredsstillende informasjonssikkerhet i kommunen
- Dersom IT-systemene blir utilgjengelige over tid (f.eks mer enn en dag) pga feil på nettverk, strømproblemer, tekniske problemer med utstyr, feil i datasystemene, brann etc, vil viktige arbeids- og beslutningsrutiner kunne stoppe opp.
- Eventuelle feil på tilgjengelig informasjon via kommunens systemer vil kunne svekke beslutningskvaliteten og bidra til spredning av feilaktig informasjon.
- Upålitelig informasjonsbehandling som følge av for dårlig tilgangskontroll, rutinefeil, driftsstans, at viktig/sensitiv informasjon kommer på avveie osv. kan medføre erstatningsansvar og dessuten skade brukernes og omgivelsenes tiltro til kommunen.

RAKKESTAD KOMMUNE
KOMMUNESTYRET

Saksbehandler Grethe Torstensen — Arkiv nr. 143 C20

Utvalg	Saknr	Møtedato
UNGDOMSRÅDET	4/11	21.11.2011
Oppvekstutvalget	4/11	23.11.2011
KOMMUNESTYRET	91/11	15.12.2011

Utvalgssak 91/11 **Saknr 11/2292** **Løpenr 14271/11**

91-11 KOMMUNEPLAN FOR IDRETT OG FYSISK AKTIVITET 2012 - 2024 PRIORITERT HANDLINGSPROGRAM 2012 - 2015

Rådmannens forslag til vedtak:

Rakkestad kommunestyre vedtar følgende "Prioritert handlingsprogram (anleggsplan) for utbygging av anlegg for idrett og fysisk aktivitet 2012:

	Tiltak	Sted	Utbygger
1.	Rehabilitering av Degerneshallen	Degernes	Rakkestadhallene AS
2.	O-kart	Haraldstad syd	Skaukam
3.	Elektroniske skiver 100m	Blytjern skytebane	Degernes skytterlag
4.	Felthurtigbane	Blytjern skytebane	Degernes skytterlag

UNGDOMSRÅDETs behandling:

Utvalgsleders forslag til uttalelse:
Utvalgsleders forslag til uttalelse er i samsvar med rådmannens forslag til vedtak.

Det kom ingen ytterligere kommentarer til forslag til vedtak.

UNGDOMSRÅDETs uttalelse :

Ungdomsrådets uttalelse er i samsvar med rådmannens forslag til vedtak.

OPPVEKSTUTVALGETs behandling:

Utvalgsleders innstilling:
Utvalgleders innstilling er i samsvar med rådmannens forslag til vedtak.

Uttalelse fra Ungdomsrådet til "*Prioritert handlingsprogram (anleggsplan) for utbygging av anlegg for idrett og fysisk aktivitet 2012-2015"* (møtedato 21.11.2011) ble lagt fram på møtedagen.

Utvalgsleders innstilling ble enstemmig vedtatt.

OPPVEKSTUTVALGETs innstilling til kommunestyret :

Rakkestad kommunestyre vedtar følgende "Prioritert handlingsprogram (anleggsplan) for utbygging av anlegg for idrett og fysisk aktivitet 2012:

	Tiltak	Sted	Utbygger
1.	Rehabilitering av Degerneshallen	Degernes	Rakkestadhallene AS
2.	O-kart	Haraldstad syd	Skaukam
3.	Elektroniske skiver 100m	Blytjern skytebane	Degernes skytterlag
4.	Felthurtigbane	Blytjern skytebane	Degernes skytterlag

Saksopplysninger:

Vedlegg:

1. Prioritert handlingsprogram 2012-2015
   A: Nærmiljøanlegg
   B: Ordinære anlegg.
2. Tabell over aktuelle utbyggingsoppgaver i et 10-12-års perspektiv.
3. Uttalelse fra Rakkestad idrettsråd.

Bakgrunn for saken:

Kommunedelplan for idrett og fysisk aktivitet 2009-2020 ble vedtatt av kommunestyret 18.12.2008. Den skal revideres hvert fjerde år. Arbeidet med ny plan starter vår 2012 og skal vedtas av kommunestyret desember 2012.

"Prioritert handlingsprogram for anlegg og områder for idrett og friluftsliv" skal rulleres og vedtas av kommunestyret hvert år. Programmet er retningsgivende ved tildeling av kommunale midler og spillemidler, og skal bl.a. vedlegges søknader om spillemidler når disse oversendes fylkeskommunen for behandling. Handlingsprogrammet må derfor være vedtatt av kommunestyret innen 15.januar, som er fristen for innlevering av søknad om spillemidler.

Kommunens ansvar for saken:

Saken skal opp i oppvekstutvalget, formannskapet og til slutt vedtas i kommunestyret.

Andre opplysninger:

Forslaget til revidert handlingsprogram for idrett og fysisk aktivitet for årene 2011-2014 er forelagt Rakkestad idrettsråd til behandling.

Nedenfor følger en kort omtale av hvert enkelt anlegg som er satt opp i handlingsprogrammet:

Nærmiljøanlegg

Aktivitetsbane ved Rakkestad ungdomsskole.

I sak 67/10, Prioritert handlingsplan for anlegg og områder 2011-2014 ble det fattet følgende vedtak i Rakkestad kommunestyre 16.12.10:

I vedlegg 1, pkt A tas følgende tiltak inn i 2012:

Ballbinge ved Rakkestad ungdomsskole Utbygger Rakkestad kommune

Det har kommet flere forslag i løpet av året om hva slags bane som skal plasseres ved ungdomsskolen:

- Ballbinge
- 7'er-kunstgressbane
- Aktivitetsbane med Sport Court dekke (velegnet til alle typer ballspill)
- Sandvolleyballbane
- Friplassen (bane for friidrett)

Det kreves en bred dialog mellom Rakkestad ungdomsskole, Rakkestad idrettsråd, idrettslaga og Rakkestad kommune for å velge et alternativ. Pr i dag er det ikke enighet om hvilken banetype som egner seg best. Prosessen må gå videre i 2012 og ev søke tippemidler i 2013.

Ordinære anlegg og rehabiliteringsanlegg

Rehabilitering av Degerneshallen
Det søkes om tippemidler til å rehabilitere tak og VVS. Søknaden ble også sent i fjor, men fikk avslag. Den sendes som fornyet søknad i år. Kostnadsramme er kr 500 000.

Rakkestadhallene AS er utbygger og det søkes midler i 2012.

O-kart Haraldstad syd
Det skal lages nytt elektronisk kart av dette området. Kartet er budsjettert med kr 165 000.

Det er Skaukam som er søker og det søkes om midler i 2012.

Blytjern skytebane – elektroniske skiver 100 m
Det er ønske om elektroniske skiver til ungdommene. Tiltaket er budsjettert til kr 540 000.

Utbygger er Degernes skytterlag og søknad sendes 2012.

Blytjern skytebane – felthurtigbane.
Det er ønske om en regional feltskytterbane på Blytjern anlegget. Tiltaket er budsjettert med kr 480 000. Det innbærer noen justeringer på nåværende anlegg.

Utbygger er Degernes skytterlag og søknad sendes 2012.

Aktuelle utbyggingsoppgaver i Rakkestad kommune i 10-12-års perspektiv

Det har kommet inn flere ønsker fra idrettslagene og de er skissert i vedlagt tabell.

Forlengelse av Dørjestien har tidligere stått på prioritert liste over utbygging. Nå står den oppført med et lengre perspektiv og er pr i dag ikke en prioritert oppgave.

Rammebetingelser:

Ved vurdering av søknader om spillemidler brukes "Bestemmelser om tilskudd til anlegg for idrett og fysisk aktivitet – 2010". Den er utgitt av kulturdepartementet.

Staten har som mål å bidra til utbygging og rehabilitering av infrastruktur, slik at flest mulig kan drive idrett og fysisk aktivitet. Det er viktig for staten å fremheve at de viktigste målgruppene for bruk av spillemidler til idrettsformål er barn (6-12 år) og ungdom (13-19 år.)

K o n s e k v e n s v u r d e r i n g e r :

Økonomi:

Det presiseres at det gjennom kommunedelplan for idrett og fysisk aktivitet ikke blir tatt noe endelig standpunkt til kommunens økonomiske deltagelse i prosjektene. Kommunal deltakelse vi alltid avhenge av kommunens økonomi og prioriteringer i årene fremover.

Imidlertid er handlingsprogrammet og kommunedelplanen et styringsverktøy for kommunen når det gjelder prioriteringer og langsiktighet i planleggingen av anlegg. Kommunens eventuelle engasjement i de enkelte anlegg vil bli behandlet i rulleringen av handlings- og økonomiplanen og de enkelte års budsjett.

Det er ikke økonomi til å gi kommunalt tilskudd til tippemiddelsøknadene for 2012.

Andre faglige vurderinger:

Rådmannen har i sitt forslag til prioritering av anlegg fulgt tidligere planer samt lagenes behov og ønsker for anlegg.

Det vises ellers til vedlagte skjematiske fremstilling av handlingsprogrammet.

Administrasjonens vurdering:

Rehabilitering av Degerneshallen prioriteres som nr 1 fordi det er lekkasjer i taket og rehabiliteringen må gjennomføres umiddelbart. Jobben er budsjettert til kr 500 000.

Skaukam har laget en meget oversiktlig liste med nylaging og revidering av kart i Rakkestadområdet. Totalt ønsker de nytegning/revidering av åtte kart. Se vedlagt tabell med et 10-12 års perspektiv.

Degernes skytterlag ønsker elektroniske skiver på 100m og utbygging av en felthurtigbane. Denne utbyggingen kan sees i et noe lengre perspektiv og de er derfor satt opp som nr 3 og 4 på prioritert liste.

RAKKESTAD KOMMUNE
KOMMUNESTYRET

Saksbehandler Knut Østby		Arkiv nr.
Utvalg	**Saknr**	**Møtedato**
Teknikk- og miljøutvalget	3/11	22.11.2011
KOMMUNESTYRET	92/11	15.12.2011

Utvalgssak 92/11 **Saknr 08/2255** **Løpenr /**

92-11 FRIVILLIG VERN AV KOMMUNESKOG - ASKEVANN

Rådmannens forslag til vedtak:
1. Rakkestad kommune aksepterer at et område på 770 daa ved Askevann i Låbyskogen vernes for all framtidig hogst.
2. Engangserstatningsbeløpet på 1 631 000 kroner aksepteres.
3. Erstatningsbeløpet blir overskuddet for Rakkestad kommunale Skoger i 2011.
4. Det arbeides videre med muligheten for frivillig vern i områdene ved Svenken og i Brattåsen.
5. Det framtidige avvirkningskvantumet i kommuneskogen skal når hele fredningsprosessen er omme tilpasses en langsiktig og bærekraftig forvaltning.

Teknikk- og miljøutvalgets behandling:

Utvalgsleders innstilling:
Utvalgsleders innstilling er i samsvar med rådmannens forslag til vedtak.

Utvalgsleders innstilling enstemmig vedtatt.

Teknikk- og miljøutvalgets innstilling til kommunestyret :

1. Rakkestad kommune aksepterer at et område på 770 daa ved Askevann i Låbyskogen vernes for all framtidig hogst.
2. Engangserstatningsbeløpet på 1 631 000 kroner aksepteres.
3. Erstatningsbeløpet blir overskuddet for Rakkestad kommunale Skoger i 2011.
4. Det arbeides videre med muligheten for frivillig vern i områdene ved Svenken og i Brattåsen.
5. Det framtidige avvirkningskvantumet i kommuneskogen skal når hele fredningsprosessen er omme tilpasses en langsiktig og bærekraftig forvaltning.

Saksopplysninger:

Vedlegg: 1. Kart over området
2. Anbefalt erstatningsforslag
3. Utkast til vernebestemmelser
4. Detaljert erstatningsberegning

Bakgrunn for saken:
Rundt 1950 ble det gjennomført et skifte av driftsopplegg i skogbruket. Da overtok flateskogbruket som driftsform på bekostning av ulike varianter av lukkede hogster. Denne endringen har etter gjeldende oppfatning medført at mange av skogens plante- dyre- og lavarter er utsatt for en større fare for utryddelse enn de var tidligere. Bakgrunnen for endringen i driftsform var at flateskogbruket medførte et mer rasjonelt skogbruk og i de fleste tilfeller en høyere produksjon – summen av dette var en bedre lønnsomhet.

Det er foretatt en vurdering av hvor mange av skogens arter som i dag regnes som truet – denne vurderingen kalles i Norge for "Rødlista". I henhold til siste oppdatering dreier dette seg om ca 1800 arter i norske skoger. Det er ikke endringen i skogbruket som er årsak til at alle disse er truet, men en antar at dette er en betydelig årsak for enkelte arter.

De fleste av disse artene vil etter forskernes oppfatning bedre sine vilkår og øke muligheten for overlevelse dersom en større andel av skogen forblir urørt og at mengden av død ved i skogene økes.

Det er fra offentlige myndigheter, skogeierorganisasjoner og miljøorganisasjoner i gangsatt ulike tiltak for å ivareta disse artene.

Fra før er kun et område lagt ut til barskogvern i Rakkestad, dette er Hiesten et område på 817 daa som ble fredet i 2002. Relativt sett er det lite fredet skog i Rakkestad kommune.

Andre opplysninger:
Det har siden vern av skog ble et tema vært strid om verdien og hensikten om dette virkemidlet. Fra skogeierhold er det hevdet at dagens skogbruk i tilstrekkelig grad ivaretar det biologiske mangfoldet, mens det fra miljøorganisasjonene blir hevdet at skogbruket må ta ansvar for mange av de artene som står på rødlista. Det er fra statlige hold vært satt et mål om total vern av ca 5 % av produktiv skog i Norge.

Følgende fire opplegg er i dag gjeldende for ivaretakelse av biologisk mangfold i skog.

1. Standard for bærekraftig skogbruk.
Ordningen er etablert som et kompromiss mellom miljøorganisasjonenes og skogeierorganisasjonenes målsettinger. Dette medfører at all virksomhet i skogbruket skal tilpasses 25 nærmere bestemte kravpunkter for å ivareta biologisk mangfold. Herunder områder som helt eller delvis er unntatt fra skogbruksvirksomhet.

2. Forskrift om bærekraftig forvaltning av skog.
Tillegg til skogloven som er mye lik standarden i pkt 1.

3. Tvungent vern av skog.

Ordningen som var det bærende prinsipp for vern av skog fram til ca 2002. Dette var en ordning hvor grunneierne fikk seg pålagt freding av skogen sin uavhengig om de ønsket det eller ikke. Denne ordningen medførte tunge og kostbare prosesser som i tillegg også bidro til streke følelser for de som var involvert.

4.Frivillig vern
Ordningen er relativt ny og innført for ha et alternativ til tvunget vern som har medført mye uro og konflikter. Frivillig vern innbærer at skogeier stiller et område til disposisjon for vernemyndighetene. Områdene blir vurdert av biologer for å få en klassifisering av hvor egnet det er for fredning. Klassifiseringen inndeles i områder med *, ** eller *** hvor områder med *** regnes som best til verneformål.

Ved frivillig vern avstår grunneier seg fra hogst i all fremtid, han beholder eiendomsretten og med det jaktretten. I tillegg beholdes andre rettigheter som kan være rettighet til bruk av veier, rydding av poster i forbindelse med jakt, oppsett av jakttårn mv. Områdene blir fredet som en kongelig resolusjon av Kongen i statsråd.

Erstatning i forbindelse med frivillig vern bygger på to prinsipper. Eldre hogstmoden skog (hkl IV og V) beregnes etter netto slakteverdi av skogen, pluss nåverdien av alle framtidige inntekter. Yngre skog beregnes etter nåverdien av de framtidige inntektene. Høyesterett har bestemt at kapitaliseringsrenten ved vern av skog skal være 5 % (som ved alle andre former for erstatninger). Ved salg av skog er det bestemt at renten skal være 4 %, dette gir en erstatning for framtidige inntekter ved salg av skog som er 20 % høyere enn ved erstatning for frivillig vern. Er gammelskogandelen høy betyr renten relativt lite. Verdivurderingen av skogen gjennomføres av en representant fra skogeiersamvirke og en representant fra staten. De legger fram et forslag til erstatning som skogeieren kan godta eller ikke.

Ordningen med frivillig vern baserer seg på en takst med relativt rause erstatninger og lite fratrekk for kantsoner og andre miljøbegrensninger. Kostnader til bygging av veier tas det også lite hensyn til. For private skogeiere er erstatningen skattefri.

Rakkestad kommune har lagt fram 3 områder for vurdering i forbindelse med frivillig vern:

- Et område på ca 770 daa ved søndre Askevann i Låbyskogen
- Et område på ca 850 daa ved det som i dag er Svenken naturreservat
- Et område på ca 310 daa vest i Brattåsen i Storetorpskogen

Alle tre områdene er klassifisert som ** områder. Dette vil si at de er interessante som fredningsobjekter.

Fredningen vil medføre noe redusert avvirkning i kommuneskogene i årene som kommer. Av de tre områdene er det kun foretatt takst i Askevannsområdet. For dette området er tilbudet om fredning lagt ut sammen med en naboskog til kommuneskogen, naboen har foreslått ca 200 daa til frivillig vern slik at det samlede arealet blir ca 1000 daa.

Kommuneskogens andel ved Askevann består av 400 daa gammelskog. Ca 1/3 av denne skogen står i et vanskelig driftsteknisk område. Det finnes noe myr i området og kommuneskogen grenser inntil to vann.

Økonomiske konsekvenser:
Verdien på området er satt til 1 631 000,-, herav er 1 419 295,- slakteverdien av påstående skog, mens kr 210 339,- er nåverdien av alle framtidige inntekter fra skog i området.

Miljømessige konsekvenser:
Vern av skog vil bidra til at biologisk mangfold ivaretas i større grad i kommunen. Dette vil også lette på kravet om at private skogeiere må verne mer skog.

Administrasjonens vurdering:
Vern av kommuneskog har tidligere blitt vurdert, det ble da fra politisk hold vedtatt at kun mindre områder i kommuneskogen skulle underlegges vern. Blant annet ble et område på 200 daa i Brattåsen vedtatt vernet. Vurderingen om at kommuneskog skulle vernes ble foretatt før de gunstige erstatningsordningene ble gjort gjeldene, dette ble derfor vurdert som for kostbart for kommunen.

Med dagens ordning stiller dette seg i et annet lys. Så lenge en får full erstatning for dagens slakteverdi og framtidige inntekter er dette et klart alternativ til å hogge gammelskog. Om en hogger får en ikke opp ny tilsvarende skog før om 70 til 130 år og da er det opp til andre å vurdere hvilke verdier det er viktig å ta vare på. Det negative med å verne i stedet for å hogge er at det blir borte noe sysselsetning i forbindelse med vern av skog.

For yngre skog er bildet noe annerledes. Høy rente gir lavere erstatninger og en ser at en her kanskje ville fått bedre utbytte ved å beholde skogen og at en på et gitt tidspunkt får en høyere tømmerpris. Men skal en få en tilfredsstillende arrondering av verneområdene må det bli med noe ungskog.

Erstatningsbeløpet er ut i fra dagens priser tilfredsstillende og vil etter dagens regelverk gi større utbytte enn salg. I tillegg beholdes eiendomsretten og med det jaktretten som også gir inntekter.

Ut i fra en helhetlig vurdering går administrasjonen i Rakkestad kommune inn for vern av kommuneskog.

Sikkerhetshåndbok for informasjons-sikkerheten i Rakkestad kommune m/sikkerhetsmål og sikkerhetsstrategi

Saksnr. 11/2248 Journalnr. 14417/11 Arkiv X57
Dato: 11.11.2011

mangfold og samhold

INNLEDNING

Denne Sikkerhetshåndboken fastlegger Rakkestad kommunes krav til beskyttelse av opplysninger som samles inn, lagres, bearbeides, overføres og formidles så vel manuelt som elektronisk.

Håndboken utgjør et felles rammeverk for det praktiske arbeid med informasjonssikkerhet i kommunen, og skal benyttes

- *for at de respektive tjenestesteder i kommunen skal kunne oppnå et nødvendig og riktig sikkerhetsnivå i sin daglige drift*
- *for å skape en felles sikkerhetskultur gjennom nødvendig opplæring og økt forståelse av behovet for informasjonssikkerhet*
- *for å etterleve kravene til informasjonssikkerhet i Personopplysningsloven og Helseregisterloven inkl Normen for informasjonssikkerhet og annet relevant lovverk*
- *som grunnlag ved meldinger til Datatilsynet*

Den enkelte leder vil være ansvarlig for at innholdet i håndboken gjøres kjent blant sine respektive ansatte – og at beskrevne, nødvendige tiltak blir iverksatt og fulgt opp.

INNHOLDSFORTEGNELSE

0. Definisjoner

Nedenfor følger forklaringer på en del viktige sikkerhetsbegrep. Denne oversikten kompletteres etter behov.

Autentisering

Autentisering innebærer nødvendig *identitetsbekreftelse* fra personell som skal ha ulik tilgang til kommunens IT-systemer og data. Normale autentiseringskrav i kommunen er *brukerident* og *passord;* ingen bruker vil få tilgang til PC, nettverk og systemer før godkjent brukerident og passord er tildelt. For å få tilgang til *personsensitive systemer/opplysninger*, kreves normalt en *ytterligere* autentisering (vanligvis ekstra passord). Passord til de respektive systemer skal også *endres* etter bestemte tidsintervall.

Autorisasjon

Med *autorisasjon* menes tildeling av *tilgangsrettigheter* til kommunens IT-systemer og data/registre. Autorisasjonen (eller *autorisasjonsprofilen*) skal angi hvilke IT-systemer, programrutiner og dataelementer vedkommende bruker har lovlig tilgang til, og hvilke operasjoner (lese, skrive, oppdatere, osv) brukeren har lov til å utføre mht dataelementene.

Autorisasjonsansvarlig

Med *autorisasjonsansvarlig* menes den person som har fullmakt til å bestemme hvilke medarbeidere som skal ha hvilke *tilgangsrettigheter* til de respektive IT-system og -behandlinger. I Rakkestad kommune er dette ansvaret lagt på *ledernivå.*

Behandlingsansvarlig

Behandlingsansvarlig er den som bestemmer formålet med kommunens behandlinger av personopplysninger og hvilke hjelpemidler som skal brukes. Behandlingsansvarlig i Rakkestad kommune er *rådmannen*.

Egenkontroller

Kommunen skal ha rutiner for kontroll av at rutiner for håndtering av personopplysninger og at *informasjonssikkerhetstiltak* er i bruk og fungerer etter hensikten på de respektive tjenestesteder.
Sikkerhetsansvarlig er ansvarlig for at egenkontrollskjema blir oppdatert etter Ledelsens gjennomgang og forøvrig ved behov i overensstemmelse med kommunens *avviks- og endringshåndtering*.

Informasjonssikkerhet

Med *informasjonssikkerhet* menes iverksettelse av planlagte og systematiske sikringstiltak i kommunen for å sikre tilfredsstillende *konfidensialitet, tilgjengelighet og integritet* spesielt knyttet til behandlingen av *sensitive personopplysninger*, og der behandlingen helt eller delvis skjer med elektroniske hjelpemidler. *Manuelle personregistre* som inneholder sensitive personopplysninger skal

også sikres på tilfredsstillende måte – og meldes til Datatilsynet *(www.datatilsynet.no).* Ref også definisjon av *'Normen'.*

Informasjonssikkerhet omfatter både *fysiske*, *organisatoriske* og *systemtekniske* sikkerhetsforhold.

Ledelsens gjennomgang

Kommunens ledelse skal jevnlig – og helst årlig – gjennomgå sikkerhetsmål og sikkerhetsstrategi for å vurdere ledelsens *beslutninger* opp mot kommunens *behov* for informasjonsteknologi og informasjonssikkerhet. Resultat fra *sikkerhetsrevisjoner* (se under) og *egenkontroller* vil danne en viktig del av grunnlaget for slike gjennomganger.

Normen for informasjonssikkerhet

Norm for informasjonssikkerhet (*Normen*) ble lansert i august 2006. *Normen* – se www.normen.no - skal bidra til tilfredsstillende informasjonssikkerhet hos den enkelte virksomhet, og i *helsesektoren* generelt. I takt med at *kommuner (*og fylkeskommuner) skal tilknyttes *helsenettet*, er det behov for en *veiledning* for disse partene, da det er mange dokumenter, lover og regler å forholde seg til. Denne veilederen – dvs *Normen* - gir førende anbefalinger og råd om hva som må ivaretas av gjeldende tekniske og administrative krav til informasjonssikkerhet når en *kommune* tilknyttes helsenettet, herunder kravene til basistjenesten som kalles *meldingsutveksling* (grunnleggende tilknytning).

I tillegg skal *Normen* bidra til å etablere mekanismer og regler som sikrer at virksomhetene kan ha gjensidig tillit til at *øvrige* virksomheters *behandling* av *helse- og personopplysninger* gjennomføres på et forsvarlig sikkerhetsnivå. Normens krav til informasjonssikkerhet er i all hovedsak overensstemmende med Datatilsynets krav til *Internkontroll*; ref Vedlegg 6 og 7.

Risikovurdering

Risikovurdering innebærer en *vurdering av effektiviteten av iverksatte sikringstiltak i forhold til mulige trusler*, og en *beskrivelse av forbedringer/nye tiltak dersom sikkerheten ikke er tilfredsstillende ivaretatt*. Eksempler på slike *trusler* kan være manglende kompetanse hos personell, svakheter knyttet til IT-systemenes tilgangskontroll, ikke god nok adgangskontroll, manglende brannsikkerhet, feil eller mangler i IT-systemer, osv. *Datatilsynet (og Normen) krever at slike vurderinger skal gjennomføres ved alle endringer som har eller kan ha betydning for sikkerheten knyttet til bruken og behandlingen av personopplysninger i kommunen.*

Samtykke

Hovedregelen knyttet til samtykke er at det skal være en *frivillig*, *uttrykkelig* og *informert erklæring* fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv. Her følger noen eksempler på samtykke – og unntak fra dette.

Helsehjelp kan bare gis med pasientens samtykke (Pasientrettighetsloven), med mindre det foreligger lovhjemmel eller annet gyldig rettsgrunnlag for å gi helsehjelp *uten* samtykke. For at samtykke skal være gyldig, må pasienten ha fått nødvendig informasjon om sin helsetilstand og innholdet i helsehjelpen.

Samtykkekompetansen kan bortfalle helt eller delvis dersom pasienten på grunn av fysiske eller psykiske forstyrrelser, senil demens eller psykisk utviklingshemming åpenbart ikke er i stand til å forstå hva samtykket omfatter. *Den som yter helsehjelp* avgjør om pasienten mangler kompetanse til å samtykke etter annet ledd. Helsepersonellet skal ut fra pasientens alder, psykiske tilstand, modenhet og erfarings-bakgrunn legge forholdene best mulig til rette for at pasienten selv kan samtykke til helse-hjelp.

Klientopplysninger i forhold til for eksempel *Lov om sosiale tjenester* skal så langt som mulig innhentes *i samarbeid med klienten* eller slik at klienten har kjennskap til innhentingen.
I saker som gjelder tjenester etter denne loven kan sosialtjenesten kreve opplysninger fra andre offentlige organer, herunder også organisasjoner og private som utfører oppgaver for stat, fylkeskommune eller kommune. Har klienten ikke samtykket i at opplysningene blir innhentet, skal spørsmålet om opplysningene kan gis uten hinder av taushetsplikt, avgjøres etter de taushetsplikt-bestemmelser som gjelder for avgiverorganet.

Sikkerhetsansvarlig

Mens rådmannen i kommunen har det overordnede, juridiske ansvaret for informasjons-sikkerheten, vil *sikkerhetsansvarlig/-koordinator* ha det sentrale, *operative* sikkerhetsansvaret i kommunen. Dette innebærer bl.a følgende ansvar og oppgaver for sikkerhetsansvarlig :

- *initiativ til sikkerhetsrevisjoner og sørge for rapportering fra disse*
- *koordinering av sikkerhetssarbeidet i kommunen og ajourhold av sikkerhetsregelverket*
- *skal påse at det foretas nødvendig sikkerhetsopplæring evt. ta initiativ til at dette gjennomføres*
- *skal påse at det ved behov gjennomføres risikovurderinger av relevante fysiske, organisatoriske og system-/IT-tekniske sikkerhetsforhold*
- *skal registrere meldinger og informere alle ledere om meldeplikten vs Datatilsynet (ref www.datatilsynet.no)*

Enhet IT ivaretar kommunens sikkerhetsoppgaver.

Sikkerhetsrevisjon

Sikkerhetsrevisjon innebærer en *etterprøving* av kommunens sikkerhetsarbeid for å verifisere at de sikkerhetstiltak som er *besluttet* etablert, faktisk *er* iverksatt og at de fungerer etter sin hensikt. Ved slik revisjon sammenlignes altså *faktisk* bruk av *informasjonssystemet* (dvs *program, data og IT-utstyr/-infrastruktur m/nettverk*) med de retningslinjer som er *besluttet*.

Ifølge *Personopplysningsloven m/forskrifter* (og *Normen*) skal slike revisjoner/kontroller gjennomføres jevnlig – og helst årlig – og skal omfatte alle enheter som behandler personopplysninger i kommunen. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som *ikke* er forutsatt, skal dette behandles som *avvik.*

Kommunen har gjennomført en sikkerhetsrevisjon i mai 2011.

Sikkerhetssoner

Datatilsynet opererer med begrepene *sikkerhetssoner*, dvs *sikker sone, intern sone og ekstern sone.* Sensitive *person*opplysninger (eks barneverns-, sosialklient- og helseopplysninger) skal som

hovedregel behandles og lagres innenfor *sikre soner* – og kun godkjent, autorisert personell skal ha tilgang til slike opplysninger. Mellom *sikret sone* og *øvrige* soner (*intern sone og ekstern sone)* skal det være installert nødvendige *sikkerhetsbarrierer,* som skal sikre at ingen ikke-godkjente tjenester skal kunne initieres fra disse soner og inn til sikret sone. Tilsvarende skal gjelde mellom intern(e)og ekstern(e) sone(r).

Men det vil også kunne forekomme behandling av sensitive opplysninger i *interne* soner; eksempel på dette er PP-relaterte elevopplysninger i skolen (eks elevinntak på spesielle vilkår), opplysninger om ansatte i kommunen, osv. Sikkerhetsmessig skal også slike opplysninger behandles på en måte som gjør at de kun skal være tilgjengelige for *autorisert* personell. Dette forutsetter igjen nødvendig sikring av konfidensialitet og integritet og skal omfatte både fysiske, organisatoriske og system-/data-tekniske sikringstiltak.

1. RAKKESTAD KOMMUNES SIKKERHETSPOLITIKK

1.1 Sikkerhetsmål

Rakkestad kommune har som sikkerhetsmål ***rett informasjon til rette vedkommende til rett tid*** *for å sikre forsvarlige tjenester til kommunens innbyggere, herunder pasienter og øvrige brukere. Dette innebærer at informasjonen må sikres tilfredsstillende*

- ***konfidensialitet –*** *slik at sensitive person-/klientopplysninger ikke blir kjent for uvedkommende, dvs at kun autorisert personell skal ha tilgang til slike opplysninger; slik tilgang skal også være sporbar/kontrollerbar*

- ***tilgjengelighet –*** *slik at alle medarbeidere med tjenestlig behov skal kunne utføre pålagte oppgaver, samtidig som brukerne av kommunens tjenester – inkl pasienter og øvrige innbyggere - gis tilfredsstillende service og informasjon.*

- ***integritet –*** *slik at opplysningene ikke utilsiktet eller uautorisert endres ved behandling. Det skal være sporbart hvem som har foretatt registreringer, endringer, rettinger og slettinger av opplysninger*

- ***kvalitet*** *– slik at sensitive helse- og personopplysninger kan henføres til riktig, identifisert person, at de registreres i henhold til avtalte regler og rutiner og at opplysningene er fullstendige, dvs resultat av autoriserte handlinger*

Sikkerhetsarbeidet i kommunen skal omfatte både ***fysiske****,* ***systemtekniske*** *og* ***organisatoriske*** *sikkerhetsforhold.*

- ***Fysisk sikring*** *innebærer i nødvendig grad å sikre kommunens tjenestesteder mot uautorisert adgang, tyveri, brann etc.*

- ***Systemteknisk sikring*** *innebærer å sikre teknologikomponentene (IT-utstyr, kommunikasjonslinjer og –utstyr/-løsninger, programvare osv.) og informasjonen (registre etc.) ved hjelp av program- og/eller maskintekniske sikkerhetsmeka-nismer/-barrierer*

- ***Organisatorisk sikring*** *fokuserer på det menneskelige element og det ansvar ledere og medarbeidere har i sikkerhetssammenheng. Sikringstiltakene kan være knyttet til administrative rutiner som ansvars- og arbeidsdeling, opplæring/motivasjon, kontrollrutiner, osv.*

- Formålet med hver *behandling* av *helse- og personopplysninger* i kommunen er å yte forsvarlig helsehjelp og tjenester knyttet til barnevern, oppvekst/kultur, økonomi, sosialytelser, osv.

- *sikkerhetsarbeidet skal ivareta hensynet til helse, miljø og sikkerhet og relevante lover og forskrifter*

- *sikkerhetsarbeidet skal rette særlig oppmerksomhet mot interne trusler/svakheter*

- *sikkerhetstiltakene skal beskytte investeringer* i teknisk utstyr og innsamlede data mot *feil, uhell, tyveri, etc*

- *sikkerhetstiltakene skal forebygge uautorisert innsyn i IT-systemer/data* og annen ikke-offentlig informasjon

- *sikkerhetstiltakene skal redusere konsekvensene* og *snarest sikre betryggende gjenoppretting til normalsituasjon* etter eventuelle feil og uhell - også eventuelle *lengre* driftsavbrudd/katastrofer

- *sikkerhetstiltakene skal sørge for at alle ledere og medarbeidere i kommunen får nødvendig opplæring i alle sikkerhetsrelaterte forhold*

1.2 Sikkerhetsstrategi

Informasjonssikkerhet i Rakkestad kommune er et *lederansvar*, men den enkelte medarbeider har et *selvstendig* ansvar for å følge vedtatte regler og vise aktsomhet i sitt daglige arbeid.

Kommunen skal ha et bevisst forhold til den risiko som gjelder ved elektronisk behandling av person-/klientopplysninger og annen viktig/sensitiv informasjon.

Kommunen er underlagt krav til informasjonssikkerhet i Personopplysningsloven m/forskrifter og i Helseregisterloven (ref *'Normen'* for informasjonssikkerhet), og er i tillegg underlagt krav om profesjonsbestemt taushetsplikt bl.a. etter Forvaltningsloven, Opplærings-loven, Barnevernloven og Helsepersonelloven. All behandling av personopplysninger skal være i samsvar med disse krav og lover.

Ved behandling av sensitive personopplysninger skal kravet til konfidensialitet ikke vike til fordel for kravet til tilgjengelighet.

Kommunen er i ferd med å etablere et *styringssystem (internkontrollsystem) for informasjons-sikkerhet;* denne håndboken med diverse vedlegg omhandler de grunnleggende *styrende, gjennomførende* og *kontrollerende* prinsipper og rutiner i dette systemet.
Styringssystemet/internkontrollsystemet er i overensstemmelse med Datatilsynets krav til internkontroll i forskriftene til Personopplysningsloven, Normen for informasjonssikkerhet og EU-direktiv 95/46 EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
Ref også http://www.datatilsynet.no/templates/article____1712.aspx og www.normen.no – og vedleggene 6 og7.

Disse kravene skal sikre at personvernet og sikkerhetsarbeidet for øvrig i kommunen blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte.

1.2.1 Organisering

Rådmannen har det *overordnede* ansvar (*behandlingsansvaret*) for informasjonssikkerheten i kommunen.

Overordnet *operativt* ansvar for informasjonssikkerheten er tillagt *sikkerhetsansvarlig;* denne funksjonen skal videreutvikle og overvåke arbeidet med informasjonssikkerhet i kommunen. Den enkelte *virksomhetsleder* har et selvstendig ansvar for gjennomføring av sikringstiltak og oppfølging av kommunens arbeid med informasjonssikkerhet.

Kommunens *informasjonssystem* (dvs den totale IT-løsning) skal konfigureres og dokumenteres slik at tilfredsstillende informasjonssikkerhet oppnås.

Bruk av IT-systemene skal skje i overensstemmelse med fastlagte rutiner, og det er den enkelte brukers ansvar å rapportere eventuelle *avvik*, eksempelvis i form av sikkerhetsbrudd, til nærmeste overordnede.

1.2.2 Partnere og leverandører

Kommunens bruk av leverandører og eventuelle partnere skal reguleres av skriftlige *kontrakter*, hvor det også skal inngå bestemmelser om *informasjonssikkerhet*. IT-systemene i kommunen driftes av IT-avdelingen.

Kommunens krav til informasjonssikkerhet ved ulike leveranser bør for øvrig dokumenteres i en egen *Kravspesifikasjon for sikkerhet (KSS).*

Kommunen skal ha kunnskap om sikkerhetsstrategien hos relevante leverandører og partnere og skal jevnlig forsikre seg om at denne strategien gir tilfredsstillende informasjonssikkerhet. Leverandør og partnere som har avgitt nødvendige erklæringer (herunder om taushetsplikt) og inngått nødvendige avtaler med kommunen, skal kunne utføre avtalt, fjernbetjent vedlikehold og oppgraderingsarbeid på kommunens IT-systemer.

1.2.3 Personellsikkerhet

Alle medarbeidere som har tjenestlig tilgang til IT-systemene skal ha nødvendige *autorisasjoner* **(**dvs rettigheter) for slik tilgang, og skal ha tilstrekkelig kunnskap om bruken av de respektive systemer og om kravene til informasjonssikkerhet.

Medarbeidere skal kun gis tilgang til sensitive personopplysninger i den grad dette er nødvendig for å utføre pålagte oppgaver, og alle medarbeidere skal være informert om den taushetplikt som gjelder. Kompetansehevende tiltak for å redusere kritisk avhengighet av nøkkelpersonell skal prioriteres.

1.2.4 Fysisk sikkerhet

Det skal treffes tiltak på kommunens tjenestesteder for å sikre mot uautorisert adgang til lokaler som ikke er åpne for publikum.

Utstyr for behandling av person-/klientopplysninger og annen informasjon som ikke skal være tilgjengelig for uautorisert personell, skal være tilfredsstillende sikret mot adgang fra uvedkommende.

1.2.5 Systemteknisk sikkerhet

Kommunens IT-systemer skal hver især inneholde mekanismer for *logisk tilgangskontroll* for å sikre at kun godkjente (autoriserte) brukere har tilgang til systemene.

IT-behandling i avdelinger og soner der det behandles *sensitive* person-/ klientopplysninger, skal være beskyttet mot innsyn fra ikke-autorisert personell.

Eksterne oppkoblinger skal kun skje i overensstemmelse med IT-avdelingen; dette omfatter også eventuell oppkobling av *hjemmekontor* og bruk av *bærbart datautstyr*.

Ved salg, kassering eller annen avhending av IT-utstyr skal det foretas forsvarlig (nødvendig) sletting av data; IT-avdelingen har ansvaret for at dette håndteres på tilfredsstillende måte.

1.2.6 Dokumentsikkerhet

Rutiner for bruk av kommunens IT-systemer og annen informasjon av betydning for sikkerheten, skal i nødvendig grad dokumenteres og være tilgjengelige på intranettet; kopier av slik dokumentasjon skal i tillegg oppbevares på annet sikkert sted ('fjernlager').

Detaljerte beskrivelser av kommunens sikringstiltak og rapporter fra risikovurderinger, sikkerhetsrevisjoner, egenkontroller og ledelsens oppfølging bør unntas offentlighet.

1.3 Hvorfor informasjonssikkerhet i Rakkestad kommune?

Kommunens økende bruk av *informasjons- og kommunikasjonsteknologi* (IKT) medfører også stor teknologisk *avhengighet og sårbarhet;* dette stiller igjen krav både til fysiske, system-/IT-tekniske og organisatoriske tiltak for å sikre kommunens informasjon, utstyr, nettverk og annen infrastruktur i tilfredsstillende grad.

Truslene mot informasjonssikkerheten kan ha sitt opphav *internt* i kommunen (medarbeidere/ utstyr/rutiner) eller skyldes *eksterne* faktorer.
De *eksterne* trusler vil etter hvert øke som følge av økt bruk av nettverkstjenester som internet etc., men de *interne trusler* bør fortsatt vies størst oppmerksomhet fordi *manglende sikkerhetsforståelse internt kan utgjøre en større trussel enn omgivelsene.*

Konsekvenser ved dårlig eller utilfredsstillende informasjonsikkerhet i kommunen:

- dersom IT-systemene skulle bli utilgjengelige over tid (for eksempel mer enn én dag) på grunn av feil på nettverk, strømproblemer, tekniske problemer med utstyr, feil i data-systemene, brann etc., vil viktige arbeids- og beslutningsprosesser kunne stoppe opp - med forsinkelser og lav effektivitet som resultat

- eventuelle feil på informasjon/data vil kunne svekke beslutningskvaliteten og bidra til spredning av feilaktige informasjoner - med mulige konsekvenser for kommunens interne og eksterne brukere – og for kommunen som sådan

- upålitelig informasjonsbehandling som følge av for dårlig tilgangskontroll, rutinefeil, driftsstans, at viktig/sensitiv informasjon kommer på avveie, osv. kan medføre erstatningsansvar og dessuten skade brukernes og omgivelsenes tiltro til kommunen

God informasjonssikkerhet blir derved en stadig viktigere forutsetning for at Rakkestad kommune skal kunne fungere tilfredsstillende og troverdig:

- hver enkelt medarbeider i kommunen har sin del av ansvaret for dette.

2 LOVER, FORSKRIFTER M.M. OG MELDEPLIKT

2.1 Lover, forskrifter og bestemmelser

For kommunens informasjonssikkerhet gjelder en rekke lover og bestemmelser som bl.a. tar sikte på å hindre at noen uten lovlig hjemmel får tilgang til personopplysninger, herunder opplysninger underlagt meldeplikt eller øvrige informasjoner unntatt offentlighet. Alle berørte ledere og medarbeidere skal gjøres kjent med og følge det til enhver tid gjeldende lovverk.

Følgende lover og bestemmelser har relevans for såvel *dokument- som databehandling* i Rakkestad kommune:

- ***Personopplysningsloven (POL)*** gjeldende fra 1.1.2001, omhandler bl.a. *meldeplikten* i forbindelse med behandling av personopplysninger. Meldinger fylles ut på meldedatabasen på www.Datatilsynet.no

- ***Forskriftene til Personopplysningsloven*****,** gjeldende fra 1.1.2001*,* omhandler bl.a. hvilke *sikkerhetsløsninger* som må iverksettes for at behandlingsansvarlig virksomhet (for eksempel Rakkestad kommune) skal ivareta kravene til konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger

- *§ 15 i* ***Lov om helseregistre og behandling av helseopplysninger*** *(Helseregisterloven) av 5. april 2001 og* ***Helsepersonelloven*** *og* ***Lov om Pasientrettigheter*** *vedrørende bl.a. behandling av klient-/pasientdata og taushetsplikt for helsepersonell*

- ***Normen for informasjonssikkerhet*** fra 28. juni 2006 med senere endringer - ref www.normen.no

- §8-8 i **Lov om sosial omsorg**, §6-7 i **Lov om barnevern** og §18-4 i **Lov om folketrygd** omhandler alle kravet om taushetsplikt

- ***Kommuneloven***

- ***Opplæringsloven***

- ***Tvangsinnfordringsloven***

- ***Lov om vergemål for umyndige***

- ***Arbeidsmiljøloven***

- ***Forvaltningsloven*** *av 10. februar 1967* inneholder bl.a. saksbehandlingsregler for forvaltningen, herunder regler om habilitet for saksbehandlere. Denne loven inneholder også regler om *taushetsplikt* (*§§13-13e),* om *informasjons- og veiledningsplikt*, om *varsling* og *innsyn* og om *klager* og *omgjøring av enkeltvedtak*

- ***Offentlighetsloven*** *av 19. juni 1970 nr 69* inneholder bestemmelser om i hvilken grad forvaltningens saksdokumenter skal være *tilgjengelige for offentligheten*. *Hovedregelen* er at dokumentene er tilgjengelige, hvis ikke denne loven eller andre lover bestemmer noe annet.

Offentlighetsloven har også en bestemmelse som sier at selv om forvaltningen kan hindre offentlig innsyn, skal det vurderes om dokumentene *allikevel* skal gjøres tilgjengelige hvis det kommer en forespørsel; dette kalles *meroffentlighet*

- ***Lov om opphavsrett*** (***Åndsverkloven***) av 12.5.1961, jfr. EU's direktiv om rettslig beskyttelse av edb-program

- ***Lov om elektronisk (digital) signatur***

- ***Straffeloven****, der bl.a. §121* omhandler kravet til *taushetsplikt* for bl.a. kommunalt ansatte

- ***Forskrift om revisjon*** av 13.01.93, spesielt § 11.2

- ***Forskrift om internkontroll - Helse, Miljø, Sikkerhet (HMS)***

- ***Løsbladforskriftenes*** bestemmelser vedrørende regnskapsinformasjon

- ***Lov om arkiv*** av 4.12.1992 og tilhørende forskrifter

- ***Sikkerhetsloven*** av 20. mars 1998, omhandler opplysninger som er av betydning for *rikets selvstendighet og sikkerhet, dvs skjermingsverdig informasjon*. Loven gjelder alle forvaltningsorgan, herunder kommuner. Loven er rettet mot å hindre at konfidensielle opplysninger kommer på avveie – ved bruk av nødvendig/aktuell sikkerhetsgrad. Loven omfatter også sikring av IT-systemer og datanett som må underlegges sikkerhetsgradering. Loven erstatter det tidligere *Datasikkerhetsdirektivet.* Følgende sikkerhetsgrader benyttes:

    - *STRENGT HEMMELIG*
    - *HEMMELIG*
    - *KONFIDENSIELT*
    - *BEGRENSET*

Øvrige bestemmelser:

- ***Personalreglementet for Rakkestad kommune***
- ***Arkivinstruks for kommunen***
- ***Anskaffelsesreglementet for kommunen***
- ***Kommunens IT-strategi***

SIKKERHETSHÅNDBOK FOR RAKKESTAD KOMMUNE

3 ORGANISATORISK SIKRING

3.1 Ansvar for sikkerheten

Rådmannen har det *overordnede, juridiske* ansvar for informasjonssikkerheten i kommunen. *Hver virksomhetsenhet har også et eget sikkerhetsansvar gjennom sine respektive ledere.*

For at den *operative* sikkerhet i kommunen skal følges godt nok opp, skal det etableres en funksjon som *sikkerhetsansvarlig;* denne funksjonen vil også ha ansvar for andre oppgaver, men skal få avsatt tid og ressurser nok til at sikkerhetsarbeidet i kommunen også får den nødvendige grad av *kvalitet og oppfølging*.

Sikkerhetsansvarlig i Rakkestad kommune er *servicekontorleder Kåre Kristiansen*.

3.1.1 Rådmannen

Rådmannen plikter å ha tilfredsstillende kunnskap om bl.a. *Personopplysningsloven* og *Helseregisterloven* og har i *sikkerhetssammenheng* det overordnede ansvaret for:

- *å etablere tiltak for **internkontroll** (styringssystem for informasjonssikkerhet)*
- *å påse at det ved behov foretas vurdering av sikkerhetsbehov og gjennomføring av nødvendige sikringstiltak i tråd med lover/forskrifter og eget sikkerhetsregelverk*
- *at det operative ansvaret for informasjonssikkerheten er definert og tilrettelagt*
- *at forholdene legges tilrette på en slik måte at alle ledere kan ivareta sitt sikkerhetsansvar*
- *at forholdene legges slik tilrette at alle medarbeidere får den nødvendige sikkerhetsforståelse og –kunnskap, slik at de kan ivareta sitt personlige sikkerhetsansvar*
- *at kommunen etterlever meldeplikten overfor Datatilsynet*

3.1.2 Sikkerhetsansvarlig

Det sentrale, *operative* sikkerhetsansvaret i kommunen skal delegeres til *sikkerhetsansvarlig* (se over*)* som bl.a tillegges følgende ansvar/oppgaver:

- *skal lede sikkerhetsrevisjoner og foreta rapportering fra disse*
- *skal sørge for at kommunens internkontrollsystem følges opp og etterleves av alle ledere*
- *skal sørge for nødvendige egenkontroller, og rapporter fra disse og ledelsens oppfølging av informasjonssikkerheten*
- *skal påse at det foretas nødvendig sikkerhetsopplæring i alle enheter og avdelinger*
- *skal påse at det ved behov gjennomføres risikovurderinger*

3.1.3 Autorisasjonsansvarlig

Autorisasjonsansvarlig er den person som har fullmakt til å bestemme *hvilke medarbeidere som skal ha hvilke tilgangsrettigheter til de respektive IT-systemer og registre.* Dette ansvaret er lagt på *ledernivå.* Autorisasjonsansvarlig skal bl.a. sørge for

- *autorisasjon til IT-systemene, dvs bestemme og registrere hvilke rettigheter medarbeidere skal ha med hensyn til å kunne registrere, oppdatere og lese informasjon i de respektive IT-system*
- *kontroll med at ingen uvedkommende får tilgang til IT-systemer og data (uvedkommende kan i denne sammenheng også være egne ansatte)*
- *å melde ut brukere ved arbeidsopphør evt. stillingsendringer*
- *at lovpålagte krav etterleves for de respektive IT-systemer og personopplysninger*

Tilgangsrettigheter tildeles via *autorisasjonsskjema*; *disse skjema er ikke gyldige uten skriftlig signatur fra autorisasjonsansvarlig*. IT-avdelingen sørger for at brukere får tilgang til nettverk og servere, mens autorisasjonsansvarlige oppretter nødvendige tilganger til *fagsystemene*.

3.1.4 IT-avdelingen

IT-avdelingen i kommunen har ansvaret for kommunens *IT-systemer*, herunder bl.a.:

- *nødvendig sikring av PC-er, nettverk, servere og øvrig, relevant IT-utstyr*
- *påse at IT-systemene med tilhørende infrastruktur tilfredsstiller alle relevante sikkerhets- og kvalitetsmessige krav i Normen for informasjonssikkerhet og forskriftene til Personopplysningsloven*
- *informasjon og opplæring/brukerstøtte knyttet til IT-systemer og sikkerhet*
- *etablering og oppfølging/kontroll av autorisasjons- og tilgangskontroll-rutiner*
- *adgangskontroll-rutiner til datarom, evt. koblingsrom etc.*
- *etablering av nødvendige planer for avbrudds-/beredskap for kommunens IT-systemer*
- *informasjon og opplæring knyttet til datarelaterte sikkerhetsforhold i kommunen*

3.1.5 Medarbeidere

Alle *ansatte og innleide medarbeidere* i kommunen skal overholde vedtatte instrukser og bestemmelser. Et effektivt sikkerhetsarbeid er avhengig av alle medarbeideres lojale holdning og aktive engasjement. Alle medarbeidere skal derfor:

- *forstå viktigheten av sikkerhet i forbindelse med eget arbeid*
- *praktisere og etterleve vedtatte sikkerhetsbestemmelser og -tiltak*
- *være ansvarlig for kvaliteten på det arbeid de utfører*
- *forstå konsekvensen ved eventuelle brudd på taushets- og sikkerhetsbestemmelsene*

Den enkelte leder har ansvaret for å følge opp at medarbeiderne får den nødvendige kunnskap og informasjon om data-/informasjonssikkerhet.

3.2 Administrative og driftsmessige sikringstiltak

3.2.1 Systemplanlegging og -anskaffelse

I forbindelse med anskaffelse av *nye* IT-systemer skal det utarbeides en *kravspesifikasjon for sikkerhet (KSS),* der krav til bl.a. systemtekniske sikringstiltak innarbeides i kravspesifikasjonen som følger tilbudsforespørselen.

Først når akseptansetest er godkjent (av ansvarlig leder/autorisasjonsansvarlig i samarbeid med IT-avdelingen), kan systemet settes i drift.

3.2.2 Drift av kommunens IT-systemer

Kommunens IT-systemer driftes av IT-avdelingen, og dette innebærer bl.a. følgende oppgaver/ansvar:

- *installasjon, overvåking og drift av IT-systemer, IT-utstyr og nettverk i nødvendig samarbeid med evt andre leverandører*
- *vurdering og implementering av nødvendige sikkerhetstiltak knyttet til IT-driften; dette vil omfatte både fysiske, organisatoriske og systemtekniske tiltak – herunder bl.a. backuprutiner, beredskapsrutiner, dataviruskontroller, nettverkssikkerhet/kryptering, nødvendig kapasitet og redundans på linjer/ nettverk, konfigurasjonsstyring, osv.*
- *brukerstøtte ved ulike feilsituasjoner*
- *oppfølging av responstider og eventuelle problemer knyttet til dette*

3.2.3 Forbedringsordning

Kommunen skal ha rutiner for rapportering, registrering og oppfølging av *feil, mangler eller avvik* – herunder forslag til mulige *forbedringer*. I denne sammenheng er dette knyttet til IT-relaterte forhold, men en slik ordning kan også tas i bruk i ulike andre sammenhenger i kommunen. I HMS-relaterte situasjoner er kommunen underlagt kravene til avviksregistrering i *arbeidsmiljøloven.*
Alle medarbeidere bør inspireres til å benytte forbedringsordningen; den bør også være tilgjengelig på kommunens *intranett.*

Avvik kan defineres som *'uønskede hendelser eller resultat som ikke er forventet eller som ikke stemmer overens med gitte spesifikasjoner'.*

Årsakene til avvik kan bl.a. være

- *feil i systemer, planlegging og/eller organisering (dvs systematiske avvik)*
- *menneskelig svikt eller feil på utstyr og/eller materiell (dvs tilfeldige avvik)*

De tilfeldige avvik kan oftest tilskrives mangelfull opplæring, dårlig arbeidsmiljø, dårlig planlegging, organisering, styring og oppfølging, dvs feil i systemer, ledelse og organisering (80% av feil som oppstår skyldes dette).

Ved eventuelle *kritiske* feil, mangler eller avvik skal det om mulig iverksettes *strakstiltak* som reduserer og forebygger skadevirkninger. Det kan være en fordel at den som oppdager eller forårsaker slike situasjoner selv registrerer det som har skjedd i en forbedringsrapport.

Forbedringsordningen skal betraktes som et *positivt læringsssignal*, og rapportene herfra må brukes konstruktivt og ikke bidra til å 'henge' ut medarbeidere. Rapporter som gjelder medarbeidere bør alltid *anonymiseres* i forhold til de informasjoner som legges ut på intranettet.

Forbedringsordningen skal motivere til at kommunen kan *lære* av de feil og avvik som oppstår, *korrigere* de feil og uønskede hendelser som inntreffer, og *forbedre* organisasjon og rutiner for å kunne *redusere* antallet feil og avvik.

Ref vedlegg 7 som eksempel på avviksrutine i kommunen.

3.2.4 Egenkontroll

Kommunen skal minst årlig gjennomføre *egenkontroll* av at rutiner for håndtering av personopplysninger og for informasjonssikkerhetstiltak er i bruk og fungerer etter hensikten ved alle tjenestesteder.

Sikkerhetsansvarlig er ansvarlig for at *egenkontrollskjema* blir oppdatert etter Ledelsens gjennomgang og forøvrig ved behov som følge av *avviks- og endringshåndtering*.

Egenkontrollskjema kan bl.a. inneholde

- *Egenkontrolltiltak – eks. vurdering av om risikobildet tilsier endrede tiltak og/eller revisjon av mål/strategi*
- *Eier av aktivitet*
- *Frekvens*
- *Resultat*
- *Kommentarer/tiltak*

3.2.5 Ledelsens gjennomgang

Kommunens ledelse skal jevnlig – og helst årlig – gjennomgå sikkerhetsmål og sikkerhetsstrategi for å vurdere ledelsens *beslutninger* opp mot kommunens *behov* for informasjonsteknologi og informasjonssikkerhet. Resultat fra *sikkerhetsrevisjoner* og *egenkontroller* vil danne en viktig del av grunnlaget for slike gjennomganger.

3.2.6 Avbrudds- og beredskapsplan

Det er en økende avhengighet av at IT-systemene i kommunen er tilgjengelige for brukerne når de trenger dem; selv korte avbrudd vil for enkelte brukergrupper innebære store ulemper/problemer. Årsakene til avbrudd kan skyldes feil på datautstyr og i datasystemer, brudd i datakommunikasjon (eksterne/interne årsaker), brann/branntilløp, strømavbrudd, etc.

For i rimelig grad å være forberedt på ulike typer avbruddssituasjoner, bør kommunen utarbeide en plan over tiltak som skal/bør iverksettes dersom det oppstår feil-/avbrudds-situasjoner. Denne planen m/tilhørende tiltak vil i stor grad også påvirke til å sikre mot IT-feil og –avbrudd - i tillegg til at de iverksatte beredskapstiltaken vil sikre at driften snarest mulig kommer igang igjen.

Her er noen momenter til avbrudds-/beredskapsplan i kommunen:

- *hvor lenge kan de enkelte avdelinger/brukergrupper være uten tilgang på viktige IT-systemer – og hvilke konsekvenser vil lengre avbrudd kunne få?*
- *oversikt over ansvarsforhold og organisering i en alvorlig avbruddssituasjon*
- *strakstiltak og aksjonering dersom ulike feil-/avbruddssituasjoner skulle oppstå:*

    - *brann, vannlekkasje, etc.*
    - *tekniske uhell/avbrudd*
    - *strømstans/overspenning*
    - *viktige data på avveie*
    - *innbrudd/hærverk/sabotasje*
    - *feil på nettverk/kommunikasjon*
    - *osv*

IT-beredskapsplan/-rutiner bør i tillegg bl.a. omfatte:

- *Backup/speiling av alle viktige IT-systemer/data – helst på atskilte lokasjoner*
- *at backup-server(e) vil være raskt tilgjengelige i en beredskapssituasjon*
- *tilfredsstillende backup-kapasitet og redundans på data-kommunikasjonslinjer*
- *avtale med dataleverandørene om rask levering etter evt. skader på eksisterende utstyr*
- *at ledere/medarbeidere og samarbeidspartnere er kjent med og tilgjengelige for å håndtere en eventuell beredskapssituasjon så raskt og riktig som mulig. Som del av dette bør det etableres et 'katastrofe-/beredskapsteam' i kommunen*
- *regelmessige penetrasjonstester (IDS – Intrusion Detection Systems) på nettverket for å avdekke eventuelle svakheter og forsøk på ikke-autoriserte tilganger (dette vil også kunne avdekke eventuelle forsøk fra interne brukere)*
- *tilfredsstillende strømforsyning, herunder god nok UPS-kapasitet for å håndtere kortere strømavbrudd – og bruk av nødstrømsaggregat for å håndtere eventuelle lengre avbrudd, overspenninger etc.*
- *automatisert driftsovervåking og alarmering (eks via sms) av temperatur, røyk, fuktighet etc. på datarom*
- *alarm-/vaktløsninger ved ulike feilsituasjoner*
- *at driftsrutiner – inkl. beredskapsplan/-rutiner - er dokumenterte på en slik måte at fravær av nøkkelpersonell ikke vil representere en kritisk faktor*
- *at dokumenterte rutiner er kjent og etterleves av relevant personell*

3.2.7 Utskrifter/dokumenter, kopiering og makulering

Utskrifter på printere skal *ikke* ligge tilgjengelig for *uvedkommende* og skal som hovedregel hentes *umiddelbart*. *Fortrolige utskrifter* skal skrives ut på printere som er plassert slik at de ikke er tilgjengelige for uvedkommende, alternativt at *'sikker print'* benyttes.

Tilsvarende regler gjelder ved *kopiering* av fortrolige utskrifter/dokumenter.

Ved utskrift av *sensitive* personopplysninger bør dette som hovedregel foretas til skrivere som kun *autoriserte* brukere/brukergrupper har tilgang til; også her vil *'sikker print'* være et godt og sikkert alternativ, da den som har en utskrift liggende i print-kø må taste eget passord på skriveren for å få aktivert egne utskrifter.

Fortrolige datautskrifter og dokumenter skal, når de ikke anvendes, oppbevares utilgjengelig for uvedkommende - og arkiveres i sikrede dokument-/arkivskap.
Fortrolige datautskrifter og dokumenter skal *ikke* kastes i papirkurv eller miljøeske, men *makuleres*.

3.2.8 Sikkerhet og orden på det enkelte kontor

Den enkelte medarbeider i kommunen har *selv* ansvaret for sikkerheten på eget kontor/egen arbeidsplass. Dette innebærer at *uvedkommende* ***ikke*** skal kunne få tilgang til ikke-offentlig informasjon, herunder viktige/sensitive *dokumenter* som måtte ligge på kontorpult.

Dette forutsetter igjen

- *at passord etc. beskyttes (dette er den enkelte ansattes egen sikkerhetsnøkkel)*
- *at PC/terminal slås av etter endt arbeidsdag – og at skjermbeskytter m/passord benyttes*
- *at viktige dokumenter, journaler, mobiltelefoner, USB-penner etc ikke ligger åpent tilgjengelige*
- *at fortrolige dokumenter ikke kastes i papirkurv, men makuleres*
- *at kontordør avlåses når kontoret ikke er bemannet; dette gjelder spesielt på steder der det foregår behandling av sensitiv informasjon og der uvedkommende vil kunne oppholde seg uten nødvendig kontroll*
- *at uvedkommende ikke har adgang til kontorlokaler når eget personell ikke er tilstede*

3.3 Personellsikkerhet

3.3.1 Etiske regler

Kommunen legger stor vekt på redelighet, ærlighet og åpenhet i all sin virksomhet.

Alle ansatte har et selvstendig *etisk ansvar* for egne handlinger, og skal ta avstand fra enhver uetisk forvaltningspraksis; eksempler på dette kan være:

- *handlinger som krenker noens rettsvern*
- *handlinger som tilgodeser noen på en uberettiget måte*

Alle ansatte plikter å overholde de etiske regler som gjelder i kommunen.

All informasjon som gis i forbindelse med virksomhet for kommunen, skal være korrekt og pålitelig og ikke med hensikt gis tvetydig formulering. Ansatte og folkevalgte skal opptre profesjonelt, med respekt og representere kommunen på en god måte både internt og eksternt.

Kollegaer:
Alle ansatte skal ta sin del av ansvaret for et godt og inkluderende arbeidsmiljø og behandle hverandre med respekt. Det forventes at det ikke snakkes nedsettende om kollegaer som ikke er tilstede og kan svare for seg. Mobbing og trakassering er ikke tillatt på noe nivå.

Innbyggere/ brukere:
Innbyggere og brukere skal møtes med respekt og høflighet. Ansatte skal opptre profesjonelt overfor brukere, og legge vekt på forsvarlig saksbehandling og sikre partenes rett til å uttale seg.

BRUK AV KOMMUNENS IT-TJENESTER

Arbeidstaker skal være meget tilbakeholden med bruk av IT-tjenestene til virksomhet som ikke har direkte tilknytning til den kommunale faglige virksomhet og administrasjon. IT-tjenestene skal ikke brukes i kommersiell sammenheng ellller til aktiviteter uten tilknytning til virksomheten som foregår i kommunen.
En arbeidstaker skal ikke benytte IT-tjenestene til å framsette ærekrenkelser eller diskriminerende uttalelser, formidle pornografi og vold, eller taushetsbelagte opplysninger, krenke privatlivets fred eller oppfordre eller medvirke til ulovlige eller rettstridige handlinger.

På digitale møteplasser og sosiale nettsteder må arbeidstaker være bevisst sin stilling og de tjenestene vedkommende yter på vegne av kommunen, og vise varsomhet og lojalitet i forhold til dette. Arbeidstakerne skal tenke gjennom konsekvensene før de publiserer noe, og være spesielt oppmerksomme på sin taushetsplikt, rutiner for intern varsling og hvem som har myndighet til, og ansvar for å uttale seg på vegne av kommunen i ulike saker

3.3.2 Fast ansatt personell og vikarer med tidsbegrenset arbeid

Medarbeidere på alle nivåer skal gjennomgå behovstilpasset opplæring i bruk av IT og i informasjonssikkerhet.

Samtlige medarbeidere skal som et minimum gis en orientering om kommunens sikkerhetsmål og retningslinjer for informasjonssikkerhet.

Kompetansehevende tiltak for å redusere kritisk avhengighet av nøkkelpersonell bør prioriteres.

Autorisasjonsansvarlig skal vurdere hvilke autorisasjoner, dvs tilgangsrettigheter vedkommende skal ha til de(t) respektive IT-system. Autorisasjonsansvarlig skal selv kunne legge inn nødvendige tilgangsrettigheter etc. i de respektive IT-systemene/applikasjonene. IT-avdelingen tildeler brukerident, passord osv.
Ved ansettelses*opphør* skal tilgangsrettigheter, passord etc *slettes umiddelbart*. Nøkler og eventuelle andre kommunale eiendeler skal innleveres.

Ved endring av stilling etc. skal også tilgangsrettighetene vurderes endret.
.

3.3.3 Konsulenter og leverandører av IT-tjenester

Alle eksterne rådgivere, konsulenter og leverandører av IT-tjenester til kommunen skal før arbeid tar til ha regulert sin tjenestetilknytning med et *kontraktsforhold; dette skal også omfatte krav til taushetsplikt*.

For konsulenter etc. som vil kunne få tilgang til *sensitive personopplysninger*, stilles det ekstra krav til konfidensiell behandling av slike opplysninger. Innleide medarbeidere og samarbeidspartnere skal ha tilgang til opplysninger etter 'need to know'-prinsippet og det skal i ettertid være mulig å foreta *kontroller* av at ingen eksterne brukere har gått ut over sine *tidsavgrensede* tilgangsmuligheter og -rettigheter.

Kommunen skal gjøre alle kontraktsparter kjent med de sikkerhetskrav og –regler som gjelder.

.

3.3.4 Servicepersonell (teknikere, håndverkere, rengjøringspersonell etc)

Servicepersonell som ikke er ansatt, men som engasjeres av kommunen, f.eks.

- *håndverkere*
- *elektrikere*
- *evt. rengjøringspersonell*
- *osv.*

skal også følge kommunens *sikkerhetsbestemmelser* i sitt arbeid for kommunen.
Uten visse regler og en viss kontroll vil risikoen for at informasjoner kan komme på avveie og muligheter for tyveri etc øke.
Det bør derfor være et overordnet prinsipp at innleid personell ikke har adgang til lokaler, utstyr og informasjoner når ansatte selv ikke er tilstede (vaktpersonale må nødvendigvis unntas fra dette kravet).

.

3.3.5 Besøkende

Kommunens ulike enheter og lokaler er i hovedsak lett tilgjengelige; dette representerer på mange måter en god, nødvendig og positiv løsning både for ansatte, besøkende/ publikum og klienter/brukere.

Samtidig behandles og lagres det informasjon i kommunen som hverken skal eller bør være tilgjengelig for uvedkommende personell. Tilsvarende gjelder datautstyr og annet utstyr.

For å sikre følsomme data, dokumenter og utstyr i nødvendig grad mot uvedkommende/ besøkende, bør derfor aktuelle kontorer på steder der uvedkommende vil kunne oppholde seg uten nødvendig kontroll, avlåses når de ikke er bemannet – også ved kortere fravær som lunchpauser etc. Kopirom og rekvisitarom etc. bør også skjermes/sikres tilsvarende.

Ved besøk, møter etc. som foregår innen soner der det behandles sensitiv personinformasjon, kan følgende besøksrutine vurderes etablert (vil ikke gjelde klienter/pårørende):

- *den som skal ha besøk får beskjed om dette*
- *den besøkende venter i resepsjonen til han/hun blir hentet av rette vedkommende*
- *etter endt besøk ledsages den besøkende tilbake til resepsjonen*

3.3.6 Taushetsplikt

Ved ansettelse i fast stilling eller vikariat i kommunen skal arbeidstaker undertegne *arbeidsavtale*, hvor ett eksemplar går til arbeidstaker og ett til arbeidsgiver; som del av arbeidsavtalen inngår også *taushetserklæring.*

Overholdelse av taushetsplikten er spesielt viktig i tilfeller der det vil kunne være til *skade* for en person dersom opplysninger om personen kommer *uvedkommende* i hende.
Med skade menes her problemer med hensyn til personlig integritet, helse, omdømme, rettigheter, osv.

Det er straffbart å bryte denne taushetsplikten etter straffelovens §121; straffen kan være bøter eller fengsel inntil 6 måneder.

Taushetsplikten gjelder også etter at ansettelsesforholdet har opphørt.

3.3.7 Brudd på reglement/arbeidsavtaler

Sikkerheten i kommunen er en svært viktig del av ansvaret til *hver enkelt arbeidstaker,* og begrensningen av risiko for feil, uhell, dårlig kvalitet, osv er nært knyttet til den enkeltes holdning og årvåkenhet, samt praktisering av gjeldende sikkerhetsbestemmelser.

For å beskytte kommunens informasjoner og øvrige verdier er det derfor av største viktighet at alle medarbeidere utviser aktsomhet i sitt arbeid.

Eventuelle brudd på disse bestemmelser skal meddeles nærmeste overordnede; slike brudd kan også få konsekvenser for arbeidstakers ansettelsesforhold i kommunen.

4 SYSTEMTEKNISK SIKRING

4.1 Sikkerhetskopiering og oppbevaring av kopier

Sikkerhetskopiering (backup) av kommunens data foretas av IT-avdelingen. De har også ansvaret for å kontrollere at sikkerhetskopieringen er *riktig* utført, og at alle data er lagt over på backup. De har likeså ansvaret for å teste 'roll-back', dvs at kopierte data kan benyttes ved eventuelle behov for rekonstruksjon etc.

Det er ikke tillatt lagret *personsensitiv* informasjon på den enkelte brukers PC/bærbare PC, mobiltelefon eller USB minnebrikke - dersom det ikke er installert *krypteringsløsninger* eller benyttes passord-løsninger for å sikre dette. *Slik lagring er den enkelte brukers eget ansvar*.

4.2 Aktivitetslogging

IT-systemene som benyttes i kommunen bør inneholde funksjoner for *logging* av aktiviteter i den utstrekning dette ansees nødvendig for å kunne *forebygge, oppdage* og *redusere skade som følge av eventuelle misbruk og feil.* For IT-systemer der det foregår behandling av sensitive personopplysninger *skal* det foretas slik logging.

Det er de respektive *autorisasjonsansvarlige* som i samarbeid med IT-avdelingen har ansvaret for å vurdere behovet for logging, etablere rutiner for dette og foreta nødvendig kontroll i ettertid.
Eksempler på relevante aktiviteter som kan/bør logges:

- *inn-/utlogging*
- *transaksjoner, sletting av data, endring av kodeverk og nøkkeldata*

Registrering av uautorisert bruk og eventuelle forsøk på slik bruk, skal ifølge Datatilsynet lagres i minst 3 måneder. Tilsvarende gjelder registrering av mulige andre hendelser som har eller kan ha betydning for informasjonssikkerheten i kommunen.

4.3 Sikringstiltak mot datavirus

IT-avdelingen har ansvaret for nødvendig sikring mot datavirus etc. på servere og nettverk. Det er scanning av evt. datavirus av all ekstern e-post til og fra kommunen på egen e-mailserver og automatisk oppdatering og 'utrulling' av antivirus-programmet til servere og klienter. Bruk av *tynne klienter* i kommunen innebærer at datavirus etc. ikke kan ramme disse 'klientene'.
På kommunens egne *bærbare* PCer etc. er det også installert nødvendig kontroll mot bl.a. datavirus og spam.
Dersom bruker oppdager eller får mistanke om datavirus, skal IT-avdelingen kontaktes umiddelbart – og PC skal *ikke* benyttes før dette er klarert.

4.4 Destruksjon av sensitive data

Ved salg eller kassering av datautstyr skal data på harddisk slettes på forsvarlig måte.
Ved disk-krasj, skal disker som inneholder følsomme data, destrueres evt. leveres til forbrenning. Datalagringsmedier skal makuleres evt. leveres til forbrenning. USB minne- pinner evt. mobiltelefoner etc. med sensitive opplysninger skal behandles på tilsvarende måte.

- *Harddisker som flyttes mellom soner eller som inneholder sensitive personopplys-ninger og skal gjenbrukes, overskrives enten med IBAS-software eller Killdisk. (www.killdisk.com)*

- *Kommmunen har etablert 'Green mobile'-løsning; denne innebærer at sensitive data på mobiltelefoner som skal kasseres, blir slettet på forsvarlig måte – og at mobiltelefonene blir kassert/destruert i henhold til de fastsatte miljøkrav*

IT-avdelingen har ansvaret for disse rutiner.

4.5 Logisk tilgangskontroll

Tilgangskontroll-rutinene skal sikre at informasjoner kun er tilgjengelig for *autorisert* personell og at de ikke *utilsiktet kan leses, endres eller slettes* ved konvertering, behandling, lagring, utskrift eller distribusjon.
Alle IT-system i Rakkestad kommune skal inneholde mekanismer for logisk tilgangskontroll, og skal omfatte nødvendig *brukeridentifikasjon, autentisering og autorisasjonskontroll.* IT-avdelingen har ansvaret for rutinene knyttet til den logiske tilgangskontrollen.

4.5.1 Brukeridentifikasjon/autentisering

Hver enkelt IT-bruker skal tildeles en unik kode for identifikasjon i forbindelse med pålogging til PC, server og nettverk.
Bruker skal logge seg ut eller 'legge ned' skjermbildet når han/hun forlater arbeidsplassen. Passord skal benyttes for å aktivisere skjermbildet.

4.5.2 Autorisasjonskontroll

Autorisasjon innebærer en godkjenning som gir brukerne tilgang til en bestemt type informasjon basert på en vurdering av de rettigheter den enkelte medarbeider skal ha.
Autorisasjonen (eller *autorisasjonsprofilen*) skal angi hvilke IT-systemer, programrutiner og dataelementer vedkommende bruker har lovlig tilgang til, og hvilke operasjoner (lese, skrive, oppdatere, osv) brukeren har lov til å utføre.
Autorisasjonskontrollen skal påse at kun autorisert personell får tilgang til IT-systemene - og kun til de program og den informasjon de er autorisert for. Tilsvarende rutiner gjelder for å unngå at brukerne kan utføre rutiner og operasjoner de *ikke* er autorisert for. Det skal i ettertid kunne foretas stikkprøvebaserte kontroller for å sikre at eventuelle forsøk på *misbruk* av tildelte autorisasjoner blir avdekket.

Det er kommunens respektive autorisasjonsansvarlige *som sammen med IT-avdelingen tildeler brukerne slike* tilgangsrettigheter. *Ved ansettelsesopphør skal rettighetene til vedkommende bruker slettes snarest.*

4.5.3 Regler vedrørende bruk av passord og påloggingsrutiner

All tilgang til kommunens IT-systemer krever brukeridentifikajon og passord; IT-avdelingen sørger for tildeling av dette ved første gangs bruk – deretter er bruker selv ansvarlig for endring og hemmelighold av eget passord.

Passordet er brukerens egen personlige *sikkerhetsnøkkel*, som skal sikre at uvedkommende *ikke* får tilgang til IT-systemene.

Følgende regler gjelder:

- *alle brukere må taste inn brukernavn og passord ved oppkobling mot PC og mot server; enkelte systemer krever i tillegg ekstra passord*
- *passord bør være minimum **6 tegn** langt og bør være en kombinasjon av tall/bokstaver*
- *passordet bør byttes hver 3. måned; ved bytte av passord skal det ikke være mulig å benytte de **5** sist brukte passord*
- *ved 3 ganger feil pålogging, skal videre forsøk sperres; brukeren må normalt kontakte IT-avdelingen for å få logget seg på igjen*
- *lån ikke bort bruker-ident eller passord; det vil i så fall være å anse som brudd på kommunens sikkerhetsbestemmelser*
- *dersom PC blir stående lengre enn f.eks. 10 minutter uten aktivitet, bør (skal) skjermbildet sperres vha av skjermsparer for å sikre mot mulig innsyn fra uautorisert personell; bruker må taste egetdefinert passord for å komme tilbake til siste skjermbilde*

4.6 Kommunikasjonssikring

4.6.1 Rutiner for kommunikasjonssikring

Kommunens rutiner for kommunikasjonssikring skal

- *sikre at kommunens nettverk, dvs utstyr og program, fungerer stabilt og med tilfredsstillende svarstider*
- *sikre at uvedkommende ikke har fysisk adgang til nettverksutstyr, modem, koblingsskap, osv. - uten nødvendig kontroll*
- *sikre at Personopplysningslovens (POL) og Normens (www.normen.no) krav til sikring etterleves, herunder kravene i den såkalte sonemodellen til Datatilsynet:*

  - ***Sikre soner*** *- for behandling/lagring av sensitive opplysninger (eks helse, barnevern, osv.)*
  - ***Intern sone*** *- for behandling og lagring av opplysninger som i hovedsak ikke skal være sensitive men som kan være i en 'gråsone' mht sensitivitet (eks PP-relaterte elevopplysninger i skolen, ansatt-opplysninger osv.)*
    - ***Eksternt nettverk/DMZ*** *- for oppkobling mot internet evt andre eksterne nettverk*

- *Mellom sikret sone og **ekstern** sone skal det minst være 2 sikkerhetsbarrierer*
- *Det er krav til **kryptering** av sensitiv informasjon som sendes over eksterne nettverk*
- *skal sikre at uautorisert tilgang til nettverk og applikasjoner ikke skjer, og at eventuelle forsøk på slik tilgang logges, oppdages og følges opp*
- *skal sikre at det finnes rutiner som snarest sikrer snarlig oppstart etter eventuelle feil/driftsavbrudd*

Nettverksløsningen i Rakkestad kommune er dermed i overensstemmelse med Datatilsynets sonemodell:

- *De '**sikre'** sonene er definert som sikre fordi datasystemene som brukes der behandler spesielt personsensitive data og som derved er underlagt sikkerhetskravene både til konfidensialitet, integritet og tilgjengelighet i POL og i Helseregisterloven/Normen for informasjonssikkerhet*
- *De **interne** sonene i kommunen benytter datasystemer som i hovedsak **ikke** behandler sensitive personopplysninger; her vil det dog også kunne foregå behandling av personopplysninger som **kan** være sensitive, derbiblant PP-relaterte opplysninger om elever i skolen, om ansatte etc. Slike opplysninger er også underlagt sikkerhets-kravene til*

konfidensialitet og integritet i POL. Brukere i intern-sone skal ikke ha tilgang til sikre soner, dvs at det ikke skal være mulig å initiere tjenester fra intern-sone mot sikker sone

- *Brukere på sikret nett som skal nå Internett må logge seg på egen, dedikert sesjon på intern sone; de vil i denne sesjonen ikke ha tilgang til de respektive fagsystemene. Brukerne har tilgang til e-post i sikker sone, men vil ikke kunne sende med **vedlegg.** Dermed har kommunen en tilfredsstillende løsning i forhold til å sikre seg mot **utilsiktet** utlevering av sensitive personopplysninger*

- *Kryptering mellom Sykehjem/sikker sone og sentral server i Rakkestad kommune foregår over Citrix ICA protokoll med "Basic encryption", som er en enkel krypteringsstandard men allikevel en fullverdig krypteringsmekanisme som skal hindre hackere i å fange opp datastrømmer i klartekst. Innholdet må også dekodes for å bli lesbart. Alle brukere i sikker sone benytter Citrix ICA for å nå sentral server og fagapplikasjoner. All datakommunikasjon i Sikker sone foregår over egen lukket fiber og kryptert trådløst radiosamband. Denne løsningen tilfredsstiller kravene til sikker (kryptert) kommunikasjon slik de er beskrevet i forskriftene til POL*

- *I de 'sensitive' fagsystemene er mulighetene for å 'klippe og lime' fjernet; dermed etterlever kommunen også kravet i POL mht. å sikre mot mulige uautoriserte endringer ('manipuleringer') av sensitive personopplysninger*

4.6.2 Bruk av elektronisk post (e-post)

Ved bruk av elektronisk post (e-post) gjelder følgende retningslinjer i kommunen:

- *e-post kan fritt brukes til meldinger som ikke inneholder sensitive/taushetsbelagte opplysninger (eks. beskjeder, meldinger, arbeidsutkast til saksdokument, møte-innkallinger, osv.)*
- *det er **ikke** tillatt å sende sensitiv informasjon via e-post (da den pt ikke krypteres)*
- *journalpliktig e-post til den enkelte ansattes e-postadresse skal registreres*
- *journalpliktig e-post som kommer til kommunens postmottak-adresse (Postmottak@rakkestad.kommune.no) skal tas ut på papir, journalføres og leveres rette vedkommende; meldingen kan i tillegg videresendes elektronisk til mottaker såfremt den ikke inneholder sensitiv, taushetsbelagt informasjon*
- *vær skeptisk til e-postsendinger spesielt med **ukjent** avsender: slike vedlegg skal **ikke** åpnes! Ved eventuelle datavirus-angrep eller ved mistanke om dette, skal datautstyr ikke benyttes før IT-avdelingen har foretatt nødvendige undersøkelser*

Kommunens rettigheter mht innsyn i ansattes e-post

E-post som er sendt og mottatt via en arbeidstakers e-postboks er *ikke uten videre* tilgjengelig for arbeidsgiver/leder. Det er imidlertid viktig å vite om arbeidsgivers rett til innsyn i e-post, hjemmeområde (H-disk) eller andre elektroniske medier. Dette gjelder også annet utstyr som er stilt for arbeidstakers disposisjon for bruk i arbeidet som PDA, mobiltelefon, minnepinne o.l. Bestemmelsene for innsyn i arbeidstakeres e-postkasse og filer reguleres av *Personopplysningsloven*.

Det er vanligvis to årsaker til at en arbeidsgiver ønsker innsyn i en arbeidstakers e-post eller filer:

1. Når det er nødvendig for å ivareta den daglige driften i virksomheten (kommunen) eller andre berettigede interesser. Eksempler på dette kan være at arbeidsgiver har god grunn til å tro at det har kommet virksomhetskritisk e-post til en arbeidstakers e-postkasse ved fravær.

2. Når det er begrunnet mistanke om at arbeidstakeren benytter e-postboksen eller arbeidsgivers utstyr på en måte som innebærer grovt brudd på arbeidsforholdet. For eksempel om arbeidsgiver har mistanke om at e-postkassen benyttes til å gjennomføre straffbare forhold.

En av forutsetningene for at innsyn kan foretas er at det er *arbeidsgiver som er eier* av utstyret eller at det er utstyr som er levert av arbeidsgiver og som benyttes under arbeid for arbeidsgiver.

Se Vedlegg 9 for ytterligere informasjon om kommunens regler for innsynsrett i e-post etc.

5 FYSISK SIKRING

5.1 Generelt

Formålet med de fysiske sikringstiltak i Rakkestad kommune er:

- *å verne om liv og helse til ansatte, klienter og andre som måtte befinne seg i kommunens lokaler*
- *å sikre eiendeler og verdier som kommunen forvalter eller formidler, herunder bygninger, lokaler, inventar, IT-utstyr og annet utstyr, mot tap eller verdiforringelse*
- *å sikre mot tap av dokumenter og elektronisk informasjon gjennom tyveri etc*
- *å hindre eller forsinke inntrenger evt. annen uautorisert adgang gjennom tilfredsstillende låsemekanismer evt. alarmsystemer*

Arealer, lokaler eller eiendeler skal ha tilstrekkelig fysisk sikring. Omfanget av de fysiske sikringstiltak bestemmes og vil være avhengig av mulige/aktuelle trusler og risiko, samt aktiviteten på stedet. De respektive ledere er hovedansvarlige for at nødvendige fysiske sikringstiltak vurderes og iverksettes på kommunens tjenestesteder.

5.2 Adgangskontroll

Adgangskontroll i kommunen innebærer nødvendig kontroll med at uvedkommende ikke kommer seg ukontrollert inn til - eller oppholder seg uten nødvendig tilsyn i – kontorsoner, tekniske rom etc. som ikke er tilgjengelige for publikum. Det skal også være nødvendig kontroll med varer og materiale som fraktes ut og inn av kommunens lokaler**.**

For øvrig gjelder følgende regler for adgangskontroll i kommunens lokaler:

- *ikke-ansatt personell skal som hovedregel **ikke** oppholde seg uten tilsyn i lokaler som ikke er åpne for publikum; dette omfatter også møtedeltakere, osv. og gjelder i kommunen generelt*

- *i kontorsoner der uvedkommende og uautorisert personell i perioder vil kunne oppholde seg, skal kontordører og dører inn til skriverrom, postrom etc. være avlåst når kontorene ikke er bemannet*
- *teknikere, håndverkere etc. skal som hovedregel alltid følges av autorisert personell fra kommunen. Tilsvarende gjelder dersom det er behov for at teknikere, håndverkere etc er tilstede i kommunens lokaler etter normal arbeidstid*

5.3 Brannsikring

Brannsikring i kommunens lokaler innebærer tiltak som skal

- *forebygge brann og branntilløp*
- *redde liv og avverge skade på person dersom brann har oppstått*
- *redusere eventuelle skadevirkninger og veilede/hjelpe medarbeidere og annet personell som oppholder seg i kommunens lokaler*
- *sørge for opplæring av medarbeidere og klienter/beboere i brannforebyggende tiltak – herunder jevnlige brannøvelser*

Ved brann/branntilløp skal evt. åpne vinduer og dører lukkes umiddelbart for å redusere lufttilførsel og dermed brannutviklingen. Mindre branner/branntilløp slokkes med håndslukkeapparat. Ved større brann- og røykutvikling skal lokalene forlates i henhold til den interne branninstruksen.

Det er installert varme-/røykvarslere med automatisk melding til 110-sentralen (Alarmsentral Brann Øst) ved utslag på disse i kommunehuset inkl serverrommet, på sykehjemmet (påbudt sikring) og på Bergenhus skole, Innbruddsalarm er koblet til samme sentral, likeså temperatur-alarm på serverrommet i kommunehuset.

Det er utarbeidet branninstrukser på alle tjenestesteder. Det er utpekt brannansvarlige på hvert enkelt sted.

Det skal jevnlig foretas brannøvelser i alle kommunale bygg.

5.4 Informasjonshåndtering

- *Datalagringsmedier i kommunen skal oppbevares slik at de beskyttes mot tyveri, skade, brann/høy temperatur, osv.*

- *Viktige og fortrolige dokumenter bør oppbevares i brann-/ vannsikre skap/rom og for øvrig sikres slik at de ikke er tilgjengelige for uvedkommende.*

6 PERSONOPPLYSNINGSLOVEN M/FORSKRIFTER og INNSYNSRETT

6.1 Personopplysningsloven

Personopplysningsloven (POL) med forskrifter trådte i kraft 1.1.2001 og gjelder for all behandling av personopplysninger der konfidensialitet, tilgjengelighet og integritet er nødvendig for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet – og der behandlingen helt eller delvis skjer med elektroniske hjelpemidler. Hovedregelen er at all slik behandling skriftlig skal *meldes* til Datatilsynet. Sensitive personopplysninger som behandles *manuelt* er også meldepliktige.

Ref pkt 2.2. side 15 vedr. kommunens oppfyllelse av meldeplikten.

Personopplysningsloven er også harmonisert med kravene i den norske og internasjonale sikkerhetsstandarden NS-ISO 27001 og EU-direktiv 95/46 EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysningerog omfatter bl.a. følgende forhold:

- *Rådmannen har hovedansvaret for at lovens og forskriftens bestemmelser følges*
- *det skal utpekes sikkerhetsansvarlig bl.a. for å kontrollere at sikkerhetskravene etterleves*
- *sikkerhetsmål og sikkerhetsstrategi skal dokumenteres og godkjennes av kommunens ledelse*
- *Det skal føres oversikt over alle personopplysninger som behandles i kommunen.*
- *Ved endringer som har betydning for informasjonssikkerheten, skal det gjennomføres* ***risikovurdering*** *av mulige interne og eksterne trusler/ svakheter knyttet til bruken av sensitive personopplysninger*
- *Det skal jevnlig (årlig) foretas* ***sikkerhetsrevisjon*** *bl.a. for å vurdere om organisering, sikkerhetstiltak og bruk av partner og leverandører er i overensstemmelse med kommunens og lovverkets sikkerhetskrav. Dersom revisjonen avdekker bruk som ikke er forutsatt, skal dette behandles som* ***avvik***
- *IT-systemene m/infrastruktur skal* ***konfigureres*** *slik at tilfredsstillende informasjonssikkerhet oppnås*
- *sensitiv informasjon som overføres over nettverk skal* ***krypteres***
- *personell som ikke er autorisert for tilgang til slik informasjon skal heller ikke ha* ***tilgangsmulighet*** *til informasjonen*
- *IT-utstyr hvor det lagres slik informasjon skal være særdeles* ***godt sikret mot adgang fra uvedkommende***

- *det skal etableres godkjente **sikkerhetsbarrierer** (fysiske/logiske) mellom de soner hvor slik informasjon behandles (=sikrede soner), øvrige soner (=interne soner) og eventuell ekstern tilknytning*

- *forsøk på uautorisert bruk skal **loggføres**, slik at det i ettertid kan foretas kontroller av eventuelle forsøk på ikke-godkjent tilgang etc.*

- *det skal etableres rutiner som fanger opp alle relevante **avvikssituasjoner** knyttet til bruken og driften av kommunens IT-systemer*

- *det skal etableres rutiner for **internkontroll***

- *forholdet til **partnere** eller **leverandører** skal reguleres i avtaler/kontrakter som også omfatter sikkerhetskrav, herunder undertegning av taushetserklæring fra alt involvert personell*

- *hvert 3. år skal meldepliktige behandlinger innrapporteres/registreres på nytt på Datatilsynets meldedatabase (www.datatilsynet.no). Dette kravet gjelder ikke for kommuner som har etablert ordning med Personvernombud*

Ref også Vedlegg 7 som omhandler Normen for informasjonssikkerhet.

6.2 Innsynsrett

I henhold til *Personopplysningsloven (POL) § 18* har kommunens egne ansatte og klienter/brukere på *skriftlig forespørsel* rett til å få opplyst hvilke informasjoner som er lagret eller som bearbeides om egen person.
Unntak fra denne innsynsretten er:

- Registre som *kun* anvendes til statistikkformål, forskning eller generelle planleggingsformål (ref. *POL §18, siste ledd*)
- Opplysninger som det må ansees *utilrådelig* at vedkommende får kjennskap til av helsehensyn eller av hensyn til forholdet til personer som står dem nær (ref. *POL §23, pkt.c*)

Svar på henvendelser om innsyn skal ekspederes snarest mulig og senest innen én – 1 måned.

Ansvarlig leder plikter å påse at taushetspliktbestemmelsene i henhold til lovverket blir fulgt i forbindelse med utlevering av opplysninger som omfattes av dette.

VEDLEGG 1 – Taushetserklæringer for ansatte i Rakkestad kommune

De til enhver tid gjeldende skjema for taushetserklæringer arkiveres sammen med sikkerhetshåndboken og blir tatt med ved senere revideringer.

Den ansatte undertegner en eller flere erklæringer etter hvilket arbeid han/hun har og derav hvilke lover vedkommende er underlagt.

Vedlegg:

- *Taushetserklæring etter Forvaltningsloven § 13*
- *Taushetserklæring etter Sosialtjenesteloven § 8 – 8 og Lov om barneverntjenester § 6 –7*
- *Taushetserklæring etter Helsepersonelloven kap. 5 og Pasientrettighetsloven*

Taushetserklæring

Rakkestad kommune

for fast ansatte og vikarer

Forvaltningen har taushetsplikt av hensyn til den som søker hjelp eller bistand, av sikkerhetshensyn, av tillitshensyn, men slik at saksbehandler får mest mulig tilgang til opplysninger som bidrar til at saken blir så godt opplyst som mulig.

FORVALTNINGSLOVEN § 13
Enhver som utfører tjeneste eller arbeider for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han/ hun i forbindelse med tjenesten eller arbeidet får vite noe om:

1- noens personlige forhold eller
2- tekniske innretninger og fremgangsmåter, samt drifts- eller forretningsforhold som det vil være konkurransemessige betydninger å hemmeligholde av hensyn til den som opplysningen angår.

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerskap, sivilstand, yrke, bopel og arbeidssted, med mindre det kan røpe et klientforhold som må anses som personlig. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal regnes som personlige, om hvilke organer som kan gi privatpersoners opplysninger som nevnt i punktum foran og opplysninger om den enkeltes personlige status for øvrig, samt vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han/hun kan heller ikke utnytte opplysningene som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

Se også på de begrensningene i taushetsplikten i fht
§ 13 a - begrensninger i taushetsplikten når det ikke er behov for beskyttelse
§ 13 b - begrensninger av taushetsplikten ut fra private eller offentlige interesser
§ 13 c - informasjon om taushetsplikt, oppbevaring av opplysninger undergitt taushetsplikt
§ 13 d - opplysninger til bruk for forskning
§ 13 e - forskeres taushetsplikt
§ 13 f - bestemmelser om taushets- og opplysningsplikt m.m. i andre lover

Som ansatt i Rakkestad kommune, erklærer jeg herved at jeg er gjort kjent med og har forstått nedenstående bestemmelser om taushetsplikt . Og at jeg som ansatt i kommunene er bundet av den taushetsplikten som følger av Forvaltningslovens § 13.<u>Overtredelse av taushetsplikten straffes etter straffeloven § 121</u>

…… navn

……. fødselsdato

…… sted/dato

…… underskrift

(Erklæringen underskrives i 2 eksemplarer, arbeidstaker beholder ett, og det andre leveres arbeidsgiver)

Taushetserklæring

Rakkestad kommune

for fast ansatte og vikarer

SOSIALTJENESTELOVEN § 8-8
Enhver som utfører tjeneste eller arbeid for sosialtjenesten eller en institusjon etter denne loven, har taushetsplikt etter forvaltningsloven §§13 til 13e.

Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerskap, sivilstand, yrke bopel og arbeidssted. Opplysning om en klients oppholdssted kan likevel gis når det er klart at det ikke vil skade tilliten til sosialtjenesten eller institusjonen å gi slike opplysninger.

Opplysninger til andre forvaltningsorganer jf. forvaltningsloven § 13 b nr. 5 og 6, kan bare gis når dette er nødvendig for å fremme sosialtjenestens eller institusjonens oppgaver, eller forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

Dersom et barns interesse tilsier det, kan fylkesmannen eller departementet bestemme at opplysninger skal være undergitt taushetsplikt, selv om foreldrene samtykker til at de gjøres kjent.
§ 8-8a - opplysningsplikt til barneverntjenesten

LOV OM BARNEVERNTJENESTER § 6-7
Enhver som utfører tjenester eller arbeider for et forvaltningsorgan eller en institusjon etter denne loven, har taushetsplikt etter forvaltningsloven §§ 13 til 13e

Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerskap, sivilstand, yrke, bopel og arbeidssted. Opplysning om en klientens oppholdssted kan likevel gis når det er klart at det ikke vil skade tilliten til barneverntjenesten eller institusjonen å gi slik opplysning.

Opplysninger til andre forvaltningsorganer jf. forvaltningsloven § 13b nr. 5og 6, kan bare gis når dette er nødvendig for å fremme barneverntjenestens eller institusjonenes oppgaver, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse. Uten hinder av taushetsplikten skal barneverntjenesten av eget tiltak gi opplysninger til sosialtjenesten når det er grunn til å tro at en gravid kvinne missbruker rusmidler på en slik måte at det er overveiende sannsynlig at barnet blir født med skade, jf lov om sosiale tjenester § 6-2 a. Også etter pålegg fra de organer som er ansvarlige for gjennomføring av lov om sosiale tjenester, plikter barneverntjenesten å gi slike opplysninger

Som ansatt i Rakkestad kommune, erklærer jeg herved at jeg er gjort kjent med og forstått overnevnte bestemmelser om taushetsplikt som følge av Sosialtjenesteloven § 8-8 og Barnevernloven § 6-7 Overtredelse straffes etter straffelovens § 121

…… …… navn
fødselsdato

…… ……
sted/dato underskrift

(Erklæringen underskrives i 2 eksemplarer, arbeidstaker beholder ett, og det andre leveres arbeidsgiver)

Taushetserklæring

Rakkestad kommune

for fast ansatte og vikarer

I følge Helsepersonelloven er alle som yter helsehjelp i form av handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål, helsepersonell.

HELSEPERSONELL LOVEN KAP.5

§ 21 Hovedregel om taushetsplikt

Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell.

§ 22 Samtykke til å gi informasjon

Taushetsplikten etter §21 er ikke til hinder for at opplysninger gjøres kjent for den opplysningen direkte gjelder, eller for andre i den utstrekning den som har krav på taushet samtykker.

§ 23 Begrensningene i taushetsplikten

§ 24 Opplysninger etter en persons død

§ 25 Opplysninger til samarbeidende personell

§ 26 Opplysninger til virksomhetens ledelse og til administrative systemer

§ 27 Opplysninger til sakkyndig

§ 28 Opplysninger til arbeidsgiver

§ 29 Opplysninger til andre formål

PASIENTRETTIGHETSLOVEN

Alle som har henvendt seg til helsevesenet med anmodning om helsehjelp, eller som helsetjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle, pasienter og har dermed krav på taushet.

§ 3-6 Rett til vern mot spredning av opplysninger

Opplysninger om legems- og sykdomsforhold samt andre personlige opplysninger skal behandles i samsvar med gjeldene bestemmelser om taushetsplikt. Opplysningene skal behandles med varsomhet og respekt for integriteten til den opplysningen gjelder.

Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker

Dersom helsepersonell utleverer opplysninger undergitt lovbestemt opplysningsplikt, skal den opplysningen gjelder, så langt forholdene tilsier det informeres om at opplysningene er gitt og hvilke opplysninger det dreier seg om.

Som ansatt i Rakkestad kommune, erklærer jeg at jeg er gjort kjent med og forstått de overnevnte bestemmelsene om taushetplikt som følger: -Helsepersonelloven kapitel 5
-Pasientrettighetsloven § 3-6

Overtredelse av taushetsplikten straffes etter straffeloven § 121

…… ……

navn fødselsdato

…… ……

sted/dato underskrift

(Erklæringen underskrives i 2 eksemplarer, arbeidstaker beholder ett, og det andre leveres arbeidsgiver)

VEDLEGG 2 - Taushetserklæring for konsulenter etc.

Taushetserklæring

Rakkestad kommune

for konsulenter og servicepersonell

Jeg forstår

- at jeg i mitt engasjement i kommunen vil kunne få tilgang til informasjon som ikke må bli kjent for uvedkommende
- at mitt engasjement i kommunen krever ansvarsfølelse og lojalitet samt respekt for vern av informasjon og øvrige verdier

Jeg forplikter meg til

- å vise aktsomhet i behandlingen av alle oppgaver jeg utfører for kommunen
- å bevare taushet om alle opplysninger og forhold jeg får kjennskap til gjennom mitt engasjement i kommunen
- vise stor aktsomhet i min omtale av kommunen

Jeg er klar over at:

- forsettlig eller uaktsomt brudd på denne taushetsplikten kan medføre straffeansvar
- taushetsplikten også gjelder etter at mitt engasjement i kommunen er avsluttet

----

Konsulent/serviceperson

Denne taushetserklæring er utstedt og underskrevet i 2 eksemplarer, hvorav hver av partene beholder hvert sitt.

Dato/sted,

----

for kommunen

Sikkerhet er DITT ansvar

12 viktige sikkerhetsregler i Rakkestad kommune

1. **du er selv ansvarlig for kvaliteten på eget arbeid**

2. **kun autorisert personell skal ha tilgang til kommunens datasystemer, dette gjelder også ved bruk av interne og eksterne nettverk (internet etc.), bærbart datautstyr og eventuelle hjemmearbeidsplasser**

3. **husk å sikre viktig/sensitiv informasjon ved bruk av bærbart datautstyr (inkl mobiltlf og USB-minnebrikker), ved oppkobling fra usikrede internettforbindelser, på reise, i kurssammenheng, osv.**

4. **passordet er din personlige 'sikkerhetsnøkkel'og skal holdes utilgjengelig for andre**

5. **logg deg ut og slå av PCen når du går for dagen; husk også at uvedkommende ikke skal se skjermbildet når du arbeider med fortrolig informasjon**

6 **la ikke fortrolige utskrifter, telefaxer, etc ligge åpent tilgjengelig**

7. **kast ikke fortrolige dokument, CDer, minnebrikker etc. i papirkurv, men makulér dem i henhold til kommunens instruks for dette**

8. **CDer, filer etc. du ikke kjenner innholdet av skal alltid kontrolleres for datavirus etc. før du tar dem i bruk og e-post-vedlegg fra ukjente avsendere skal ikke åpnes**

9. **piratkopiering av programvare er forbudt i henhold til Lov om opphavsrett**

10. **uvedkommende skal ikke uten nødvendig kontroll ha adgang til steder hvor datautstyr, skrivere etc. er plassert**

11. **snakk ikke om følsomme, virksomhetsrelaterte saker til uvedkommende, herunder opplysninger om klienter og beboere**

12. vær årvåken i det daglige arbeid - og si fra om noe unormalt oppdages

VEDLEGG 4 – Generelle regler for bruk av internet

RAKKESTAD KOMMUNE

Generelle retningslinjer for bruk av internet

- ***Bruk internet til nyttige og jobbrelaterte formål***
- ***Det skal vises respekt for andre personers livssyn, nasjonalitet og rase, og andre personer skal ikke forulempes eller fornærmes; dette gjelder også for sosiale medier som Facebook o.l.***
- ***husk å sikre viktig/sensitiv informasjon ved oppkobling fra usikrede internettforbindelser, på reise, i kurssammenheng, osv.***
- ***Det skal ikke lastes ned, søkes tilgang til eller spres pornografisk, voldelig, rasistisk eller blasfemisk materiale***
- ***Husk at du på internet er en synlig representant for kommunen og at du setter spor på alle nettsider du besøker***
- ***Dokumenter eller annen informasjon som inneholder personopplysninger og som er underlagt regulatoriske krav, skal ikke sendes over nettet. Det samme gjelder informasjon du ikke er sikker på kan offentliggjøres***
- ***Det skal ikke sløses med ressurser på nettet. Unødig surfing, sending av e-post (, videoopptak, masseutsendinger etc.) og annet skal unngås***
- ***Ved mistanke om datavirus skal IT-avdelingen kontaktes umiddelbart og PC etc. skal ikke benyttes***
- ***Nedlasting av programvare skal begrenses. Det er ikke lov å lagre eller kjøre/laste ned programvare som ikke er godkjent av IT-avdelingen. Nedlasting av programvare uten gyldige lisenser er likeledes ikke tillatt***

- ***Vær oppmerksom på at bilder, lyd og tekst kan være belagt med kopirestriksjoner. Å laste ned eller videresende slikt materiale er ikke tillatt uten at godkjennelse for dette er innhentet***

- ***Dersom det oppdages ulovlig bruk av nettet, skal dette varsles nærmeste overordnede***

VEDLEGG 5 – Sikring av hjemmearbeids-PCer etc.

Spesielle krav til sikring av hjemmearbeids-PCer og bærbart datautstyr

Hjemmearbeids-PCer etc. som benyttes til jobbrelaterte oppgaver skal som hovedregel behandles og sikres på lik linje med tilsvarende utstyr på kommunens arbeidsplasser. Slik bruk bør i all hovedsak også foretas på *separate* PC; dette gjelder spesielt dersom det unntaksvis foretas behandling av sensitive opplysninger/personopplysninger.

Bruk av hjemmearbeids-PCer og bærbare PCer er ennå lite utbredt i kommunen, men slik bruk vil gradvis øke. Derfor er det utarbeidet noen generelle råd om relevante sikringstiltak for bruk av slikt utstyr (ref her også www.nettvett.no) :

- *hjemmearbeids-PC og bærbare PCer skal ikke tas i bruk til jobbrelaterte oppgaver før nærmeste overordnede og IT-avdelingen har gitt sin godkjennelse til dette*

- *passord skal benyttes og endres i overensstemmelse med kommunens regler for dette*

- *dersom det arbeides med opplysninger som er underlagt Personopplysningsloven etc., skal slikt utstyr i hovedsak ha en sikkerhet som i størst mulig grad samsvarer med sikkerheten på tilsvarende arbeidsplass i kommunen*

- *det er ikke tillatt å **lagre** sensitive personopplysninger på hjemmearbeids-PCer og bærbart utstyr, og **bruk** av slike opplysninger skal kun skje i samråd med autorisasjonsansvarlig og IT-avdelingen*

- *ved bruk av internet og e-post fra slikt utstyr, bør (skal) det installeres krypterings-/ brannmurløsninger dersom det arbeides med følsomme informasjoner; IT-avdelingen vil bistå med å få vurdert, anskaffet og installert dette*

- *det skal installeres programvare for sikring mot datavirus; sørg også for at antivirusprogrammet oppdateres jevnlig; IT-avdelingen vil gi råd og bistå her*

- *vær skeptisk til e-postsendinger spesielt med **ukjent** avsender: ikke åpne vedlegg fra slike! Ved eventuelle datavirus-angrep eller ved mistanke om dette, skal ikke utstyret benyttes før IT-avdelingen har foretatt nødvendige undersøkelser*

- *slå av strømmen på datautstyr når det ikke er i bruk; på bærbare PCer er det ikke nok å lukke lokket og la PCen stå i hvilemodus: ved et mulig tyveri vil dette muliggjøre enkel tilgang til det som er lagret på PCen dersom kryptering ikke benyttes*

- *sørg for tilfredsstillende fysisk sikkerhet rundt bruken og oppbevaringen av datautstyret; dette gjelder også USB minnebrikker etc. Bærbart datautstyr bør sikres på best mulig måte i forhold til tyveri etc; slikt utstyr bør aldri forlates dersom uvedkommende er i nærheten. Det bør heller ikke forlates lett synlig i bil etc. På flyreiser etc. bør datautstyr du ikke bærer på deg tas med som håndbaggasje – og holdes under oppsyn. Vær også OBS ved bruk og oppbevaring av slikt utstyr på møterom, hotellrom, på konferansesteder, osv.*

- *det er ikke tillatt å benytte piratkopiert programvare i kommunen; dette gjelder selvsagt også på hjemmearbeids-PCer og evt. bærbart datautstyr*

- *backup av viktige program og datafiler bør tas jevnlig også på hjemmearbeids-PCer – og lagres på betryggende måte*

- *hjemmedata-utstyr (og for øvrig alt annet elektrisk og elektronisk utstyr) skal alltid tilkobles jordet kontakt*

- *ha lett tilgang til brannslokningsutstyr (håndslokkeapparat) på hjemmearbeidsplassen – og i hjemmet for øvrig*

- *hjemmearbeidsplasser bør i rimelig grad - og avhengig av bruk/hva det arbeides med - avskjermes i forhold til uvedkommende (også andre familiemedlemmer)*

For ytterligere råd knyttet til hjemmekontor- og bærbart datautstyr, gjengis nedenfor **Datatilsynets egen, interne instruks for bruk av hjemmekontorutstyr:**

- *Det skal ikke behandles eller lagres sensitive personopplysninger på slikt utstyr.*
- *Saksdokumenter skal ikke varig lagres på lokal disk på hjemmekontor. Lagring utover 60 døgn skal begrunnes.*
- *Det skal brukes brukernavn og passord for å få tilgang til hjemmekontorutstyr*
- *Det skal ikke installeres programmer på datamaskinen uten at det er godkjent av systemansvarlig*
- *Det skal til enhver tid benyttes antivirusprogram. Dette skal jevnlig oppdateres og kjøres*

VEDLEGG 6 - Rutiner for Internkontroll

Internkontroll-rutiner i Rakkestad kommune

Rutinene for internkontroll skal i hovedsak sikre rettighetene til 3. part, dvs den registrerte selv. Kravene til slik internkontroll er definert i Personopplysningslovens (POL) § 14 og nærmere spesifisert i kapittel 3, §3-1 i forskriftene til loven.

Tiltakene skal tilpasses*'kommunens art, aktiviteter og størrelse og i det omfang det er nødvendig for å etterleve kravene i loven'* slik det står beskrevet i forskriftene.

For Rakkestad kommune vil de tiltak som iverksettes for å sikre informasjonssikkerheten, sammen med øvrige rutiner knyttet til behandling av personopplysninger i kommunen, i all hovedsak også dekke de nedenstående kravene til et internkontroll-system, som består av:

- ***Styrende dokumentasjon (mål/strategi, ansvar/myndighet, organisering osv.)***
- ***Gjennomførende dokumentasjon (prosedyrer og instrukser)***
- ***Kontrollerende dokumentasjon (rapporter, sjekklister, logger, osv.)***

Internkontrollen i kommunen innebærer at:

- *Rådmannen og virksomhetslederne har den nødvendige kjennskap til gjeldende regler for behandling av personopplysninger*
- *Tiltak for å sikre tilfredsstillende behandling av personopplysninger dokumenteres; denne dokumentasjonen skal være tilgjengelig for de den måtte angå*
- *Det er etablert rutiner for å oppfylle de registrertes rettigheter, herunder rutiner for*
  - *innhenting og kontroll av de registrertes samtykke, jfr. POL §§ 8, 9 og 11*
  - *vurdering av formålet med behandling av personopplysninger i samsvar med POL § 11a*
  - *vurdering av personopplysningenes kvalitet i forhold til det definerte formålet, samt oppfølging av eventuelle avvik*
  - *oppfyllelse av begjæringer om innsyn og informasjon, jfr. POL §§ 16 til 24*
  - *oppfyllelse av krav fra den registrerte om reservasjon mot visse former for behandling av personopplysninger, jfr. POL §§ 25 og 26*
  - *oppfyllelse av lovens regler om meldeplikt, jfr. POL §§ 31- 33*
- *leverandører som måtte få tilgang til personopplysninger på oppdrag fra kommunen, skal behandle slike opplysninger i samsvar med inngåtte avtaler, kravene i Person-opplysningsloven og med kommunens rutiner for dette*

VEDLEGG 7 - Normen for informasjonssikkerhet

Normen for informasjonssikkerhet – www.normen.no – omhandler et styringssystem for informasjonssikkerhet. I all hovedsak er dette systemet i overensstemmelse med kravene til internkontroll definert i Personopplysningslovens (POL) § 14 og nærmere spesifisert i kapittel 3, §3-1 i forskriftene til POL – ref Vedlegg 6. Kommunens fokus på informasjonssikkerhet og ulike sikkerhetstiltak har som en overordnet målsetting å etterleve såvel Datatilsynets som Normens krav til internkontroll og sikkerhetsstyring. Pr juni 2011 er hovedtyngden av disse krav implementert i Rakkestad kommune.

Her er hovedpunktene i 'normen:

- Kommunens ulike sikkerhetstiltak/styringssystem for informasjonssikkerhet skal sikre at personvernet og sikkerhetsarbeidet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte. Systemet omfatter en *styrende*, en *gjennomførende* og en *kontrollerende* del – i samsvar med Datatilsynets internkontroll-krav

1. Styrende del

- *Beskrivelse av ledelse og organisering av informasjonssikkerhet*
- *Beskrivelse av og oversikt over formålet med behandlingene*
- *Fastsettelse av sikkerhetsmål og -strategi*
- *Fastsettelse av nivå for akseptabel risiko*

2. Gjennomførende del

- *Prosedyrer*
- *Dokumentasjon av sikkerhetstiltak*
- *Opplæring*

3. Kontrollerende del

- *Risikovurdering*
- *Sikkerhetsrevisjon*
- *Avvikshåndtering*
- *Ledelsens gjennomgang*

1.1 Organisering og styring av informasjonssikkerhet

- *Ansvarsforhold beskrives slik at det er tydelig hvem som er ansvarlig på ulike nivåer og hva de er ansvarlig for (hva dette ansvaret innebærer)*
- *Formål med behandling av helse- og personopplysninger beskrives slik at det er tydelig hva helse- og personopplysningene benyttes til*
- *Mål for informasjonssikkerhet defineres. På grunnlag av målene skal det fastsettes et nivå for akseptabel risiko (akseptkriterier) slik at det er mulig å kontrollere om sikkerhetsmålene nåes*
- *Strategien skal vise valg og prioritering av sikkerhetstiltak*

2.1 Gjennomføring

- *Det skal føres oversikt over helse- og personopplysninger som behandles i virksomheten.*
- *I oversikten skal hjemmelsgrunnlaget for behandlingen angis og tidspunkt for når melding evt. konsesjonssøknad er sendt Datatilsynet*
- *Oversikt over partnere og leverandører skal dokumenteres. Virksomheten skal etablere klare ansvarsforhold mellom partnere og leverandører som beskrives i en særskilt avtale*
- *Konfigurasjonskart og beskrivelse av den IT-tekniske løsningen skal utarbeides. Løsningen skal baseres på valgt sikkerhetsstrategi og risikovurderinger*
- *Prosedyrer for informasjonsbehandlingen skal dokumenteres og innføres*
- *Risikovurderinger skal gjennomføres for å kartlegge risikoområder og klarlegge*
- *sannsynligheten for og konsekvens av uønskede hendelser (sikkerhetsbrudd). Hver enhet og hvert nivå ved respektive ledelse skal gjennomføre risikovurderinger periodisk og etter fastsatte maler og retningslinjer.*
- *Risikovurdering skal som minimum gjennomføres før*

    - *etablering av nye informasjonssystemer eller registre som inneholder helse- og personopplysninger*
    - *organisatoriske endringer som kan påvirke informasjonsbehandlingen*
    - *større konfigurasjons- og systemendringer*

3.1 Kontroll og oppfølging

- *Ledelsen skal utarbeide og vedta en plan for risikovurderinger*
- *Ledelsen skal foreta kontroll av risikovurderingene og påse at resultatet av risikovurderingene er i henhold til fastlagte akseptkriterier*
- *Sikkerhetsrevisjoner skal gjennomføres jevnlig og minimum årlig. Ledelsen skal utarbeide og vedta en plan for sikkerhetsrevisjoner i virksomheten*
- *Avvikshåndtering iverksettes ved sikkerhetsbrudd og/eller når oppgaver utføres i strid*
- *med gjeldende prosedyrer eller "vanlig praksis". Virksomheten skal ha en egen prosedyre for håndtering av avvik*
- *Ledelsens gjennomgang skal gjennomføres iht utarbeidet møteplan. Formålet med ledelsens gjennomgang er å avdekke om sikkerheten ivaretas iht mål, strategier og prosedyrer og beslutte handlingsplaner for det videre sikkerhetsarbeidet. Ledelsens gjennomgang skal gjennomføres minimum årlig og i sammenheng med årlig økonomi- eller virksomhetsplanlegging*

VEDLEGG 8 - Rutine for avviksbehandling i Rakkestad kommune

(omfatter bruk/administrasjon av IT-systemer/informasjonssystemer)

Rutine for avviksbehandling i Rakkestad kommune

Formål

Denne rutinen skal sikre at uregelmessigheter i bruk eller administrasjon av kommunens IT-systemer som skyldes brudd på sikkerhet, eller mistanke om brudd på sikkerhet, blir gjenstand for rapportering, gransking og utbedring.

Rutinen skal benyttes ved alle typer brudd på sikkerhet/informasjonssikkerhet i kommunen.

Ansvar og myndighet

Det er kommunens *sikkerhetsansvarlig* som er ansvarlig for denne avviksrutinen – og for eventuelle *endringer* i denne.

Sikkerhetsansvarlig er også ansvarlig for vedlikehold av rutinen og for godkjenning av eventuelle tilpasninger.

Aktivitet	***Ansvar/utførende***
Definisjoner og eksempler *<u>Avvik</u>* *1. Manglende samsvar mellom det som faktisk skjer og det som er beskrevet i kommunens Retningslinjer for informasjonssikkerhet* *2. Uønskede hendelser som er et brudd på eller kan innebære en fare for brudd på informasjonssikkerheten* *<u>Avviksbehandling</u>* *Systematiske tiltak for å fjerne årsaken til feil eller mulige sikkerhetsbrudd* *Eksempler på avvik knyttet til informasjonssikkerhet:* - *utilsiktet utlevering av personopplysninger* - *forsøk på bruk av IT-systemer uten nødv. autorisasjon* - *oppgaver utført i strid med gjeldende rutiner* - *forsøk på uautorisert inntrenging (hacking etc.) i IT-systemene* - *bruk av konsulenter etc. uten godkjent kontrakt* - *angrep av datavirus*	

Aktivitet	***Ansvar/utførende***
1. Strakstiltak ved oppdagelse av avvik	
Den som oppdager et avvik, foretar de strakstiltak som er mulige – om nødvendig i samarbeid med nærmeste overordnede	Alle ansatte
Dersom en uilsiktet hendelse kan berøre andre ansatte/avdelinger, skal disse varsles snarest mulig.	Alle ansatte
2. Start avviksrapport	
Den ansatte som oppdager et avvik, skal snarest rapportere dette i den form/på den måte som til enhver tid gjelder. *Rapport skal leveres avdelingsleder.*	Alle ansatte
Alle avviksrapporter skal unntas offentlighet etter Off.lovens § 6.2a.	
Vurdering og gjennomføring av ytterligere strakstiltak skal skje umiddelbart etter mottak av rapport eller annet varsel	Avdelingsleder
3. Analyse og korrigerende tiltak	
Avdelingsledelse informerer sikkerhetsansvarlig og øvrig ledelse om hendelsen.	Avdelingsleder
Avdelingsledelse iverksetter nødvendig vurdering/analyse av årsaksforhold og evt. ytterligere korrigerende tiltak.	Avdelingsleder
Om nødvendig gjennomføres en risikovurdering basert på den aktuelle hendelsen.	Avdelingsleder
4. Rapportering	
Kopi av ferdig utfylt rapportformular sendes sikkerhetsansvarlig.	Avdelingsleder
Dersom et sikkerhetsbrudd har ført til uautorisert utlevering av personopplysninger (eks. feil mottaker eller feil informasjon) eller det er mistanke om slik utlevering, skal Datatilsynet ha melding om dette avviket. *Sikkerhetsansvarlig skal ha kopi av denne meldingen*	Avdelingsleder
5. Etterkontroll	
Det skal etter en tid foretas etterkontroll av iverksatte tiltak for å få bekreftet at disse fungerer som forutsatt. *Tidsintervall mellom hendelse og etterkontroll bestemmes av hendelsens art.*	Avdelingsleder
6. Endring av regelverk	
Dersom en avviksregistrering kan tyde på at det eksisterende regelverk bør justeres, skal sikkerhetsansvarlig ha melding om dette.	Avdelingsleder
Sikkerhetsansvarlig skal vurdere og evt. ta initiativ til aktuelle endringer	Sikkerhetsansvarlig

Aktivitet	***Ansvar/utførende***
7. Dokumentasjonskrav	
Avviksbehandling skal kunne dokumenteres i en rapport som inneholder disse elementene: - *dato/tid/sted for avviket* - *hvem rapporterer* - *opplysninger om selve avviket* - *utførte strakstiltak* - *årsaksanalyse* - *korrigerende tiltak basert på årsaksanalyse/-vurdering* - *resultat fra etterkontroll* - *oversikt over hvilke medarbeidere som har vært involvert i avviksbehandlingen* *Det er utarbeidet et eksempel på skjema for avviksrapportering og behandling – se neste side, skjema Avviksrapport*	Avdelingsleder
8. Statistikk	
Den enkelte avdeling skal føre en samlet oversikt over avvikshendelser innenfor eget ansvarsområde.	Avdelingsleder
Sikkerhetsansvarlig skal ha en samlet oversikt over alle hendelser innen kommunen.	Sikkerhetsansvarlig
Statistikk skal periodisk analyseres for å vurdere om det er et mønster i hendelser som bør medføre nye sikringstiltak eller reaksjoner *For avdelingen foretas slik analyse av avdelingsleder.*	Avdelingsledelse
For kommunen totalt skal slik analyse foretas av sikkerhetsansvarlig	Sikkerhetsansvarlig
9. Ledelsens gjennomgang	
Samlerapport over avvik og statistisk materiale skal forelegges ledelsen minst en gang pr år i forbindelse med andre vurderinger av sikkerhetstiltak og dokumentasjon.	
Sikkerhetsansvarlig påser at dette blir gjort for kommunens ledelse.	Sikkerhetsansvarlig

Resultatdokumenter

- Rapport fra avviksbehandling. Arkiveres i lokalt saksarkiv
- Statistisk materiale. Arkiveres hos hhv. avdelingsleder og sikkerhetsansvarlig
- Evt. meldinger til Datatilsynet. Arkiveres hos avdelingsleder

Referanser

- Rutine for ledelsens gjennomgang
- Rutine for dokumentasjonskontroll
- Datatilsynet: Personopplysningsloven m/forskrifter gjeldende fra 01.01.2001
- Skjema for avviksrapportering

Avviksrapport i Rakkestad kommune

Utfylt rapport skal unntas fra offentlighet etter Off.lovens § 6.2a.

For behandling av rapport, se ***Rutine for avviksbehandling***.
Hvis plassmangel, lag en henvisning og bruk vedlegg.
I høyre kolonne påføres navn på den/de som deltar i aktiviteter under behandlingen av avviket.

Virksomhet/avdeling:

Aktivitet	***Navn***
Rapportinformasjon *Navn på melder:* *Dato/tid/sted:* *Evt. maskinident:* ***Beskriv avviket****:* ***Årsaksanalyse/-vurdering:*** *Når foretatt:* *Av hvem:* *Resultat:* ***Tiltak iverksatt etter årsaksanalyse:*** ***Rapport til Datatilsynet? (Ja/Nei):*** ***Etterkontroll:*** *Fastsatt til (dato/tid):* *Foretatt (dato/tid):* *Resultat:*	

Arbeidsgivers innsynsrett i e-post m.m.

Informasjon om arbeidsgivers innsynsrett.

E-post som er sendt og mottatt via din e-postboks er ikke uten videre tilgjengelig for din arbeidsgiver, eller for din leder. Det er imidlertid viktig å vite om din arbeidsgivers rett til innsyn i din e-postkasse, hjemmeområde (H-disk) eller andre elektroniske medier. Dette gjelder også annet utstyr som er stilt for arbeidstakers disposisjon for bruk i arbeidet som PDA, mobiltelefon, minnepinne o.l. Bestemmelsene for innsyn i arbeidstakeres e-postkasse og filer reguleres av personopplysningsloven.

Det er vanligvis to årsaker til at en arbeidsgiver ønsker innsyn i din e-post eller i dine filer:

1. Når det er nødvendig for å ivareta den daglige driften i bedriften eller andre berettigede interesser. Eksempler på dette kan være at arbeidsgiver har god grunn til å tro at det har kommet virksomhetskritisk e-post til din e-postkasse ved ditt fravær.

2. Når det er begrunnet mistanke for at arbeidstakeren benytter e-postboksen eller arbeidsgivers utstyr på en måte som innebærer grovt brudd på arbeidsforholdet. For eksempel om arbeidsgiver har mistanke om at e-postkassen benyttes til å gjennomføre straffbare forhold.

En av forutsetningene for at innsyn kan foretas er at det er arbeidsgiver som er eier av utstyret eller at det er utstyr som er levert av arbeidsgiver og som benyttes under arbeid for arbeidsgiver.

Det er Personopplysningsforskriften som definerer virkeområdet.
Personopplysningsforskriften §9-1:
Med arbeidstakers e-postkasse menes e-postkasse arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten. Reglene gjelder tilsvarende for arbeidsgivers adgang til gjennomsøking av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet ved virksomheten. Bestemmelsene gjelder også for arbeidsgivers innsyn i opplysninger som arbeidstaker har slettet fra de nevnte områdene, men som finnes lagret på sikkerhetskopier eller lignende som arbeidsgiver har tilgang til.

Reglene gjelder både overfor nåværende og tidligere arbeidstakere, samt andre som utfører, eller har utført, arbeid for arbeidsgiver.

Når arbeidsgiver skal gjennomføre innsyn i arbeidstakers e-postkasse eller filer må arbeidsgiver følge et sett med retningslinjer:

- *Arbeidstaker skal så langt som mulig varsles og få anledning til å uttale seg før arbeidsgiver gjennomfører innsyn.*
- *Varslet skal inneholde begrunnelse for hvorfor vilkårene for innsyn anses å være oppfylt og orientere om arbeidstakers rettigheter etter forskriften.*
- *Arbeidstaker skal så langt som mulig gis anledning til å være tilstede under gjennomføringen av innsynet, og har rett til å la seg bistå av tillitsvalgt eller annen representant. Arbeidstaker kan fritt avstå fra å være tilstede.*
- *Innsyn skal alltid gjennomføres med minst 2 personer tilstede.*
- *Innsyn må gjennomføres på en slik måte at dataene så lang som mulig ikke endres og at frembrakte opplysninger kan etterprøves.*
- *Dersom innsyn i e-postkassen viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i etter vilkårene, skal e-postkassen og dokumenter i denne straks lukkes. Eventuelle kopier skal slettes.*

Dersom en arbeidsgiver foretar innsyn uten varsel, for eksempel om den ansatte ikke er mulig å få tak i, eller tidsaspektet tilsier at man ikke rekker å varsle før et evt. innsyn må foretas skal den ansatte underrettes i etterkant.

Underretningen skal, i tillegg til informasjon om vilkårene som er ansett oppfylt, inneholde opplysninger om hvilken metode for innsyn som ble benyttet, hvilke e-poster eller andre dokumenter som ble åpnet samt resultatet av innsynet.
Her er noen råd og anbefalinger til deg som arbeidstaker:

- *privat bruk av kommunens e-postsystem bør begrenses til et minimum. De ansatte oppfordres til å bruke privat e-post til private ting og kommunens e-post til offentlige meldinger, så langt dette er mulig.*
- *merk private e-poster med "privat" eller lagre disse i separate mapper slik at det tydelig fremkommer at disse er privat.*
- *husk at alt du foretar deg på arbeidsgivers datasystem kan spores tilbake til deg.*

INNSYNSRAPPORT RAKKESTAD KOMMUNE

Hvem ble det foretatt innsyn hos (fullt navn):	
Navn på tilstedværende under innsynet	**Enhet/funksjon**
1.	
2.	
3.	
Innsynet ble foretatt:	
Dato	
Sted	
Fra kl.	**Til kl.**
Oppsummering av innsynet (Hva ble det foretatt innsyn i ?) *	
Øvrige kommentarer:	

Sted og dato	**Underskrift av de som var tilstede**:

*** F.eks. hvilke dokumenter ble åpnet eller skrevet ut ? Ble de kopiert over til fellesområde ?**
Metodebruk, f.eks. ble det søkt etter stikkord og/eller dato? Hvorvidt man fant det man så etter..?

Den det ble foretatt innsyn hos skal ha kopi av rapporten.

INNSYNSBEGJÆRING RAKKESTAD KOMMUNE

Innsyn begjæres av:	
Hvem skal det begjæres innsyn hos:	
Innsynet begjæres i: **Virksomhetsrelatert e-post** ☐ **Virksomhetsrelatert dokumenter på h-disk** ☐ **Mobiltelefon/minnepinne** ☐ **Annet** ☐ **Spesifiser**:_____	
Begrunnelse for begjæringen/formålet med innsynet:	
Gis den ansatte informasjon i forkant: **JA** ☐ **NEI** ☐	
Hvis NEI – oppgi begrunnelse:	
Sted og dato:	**Underskrift**:

Vedlegg 1 til Kommuneplan for idrett og fysisk aktivitet 2009 – 2020 – Rakkestad kommune.

Prioritert handlingsprogram 2012 – 2015
Utbygging og tilrettelegging av anlegg og områder for idrett og friluftsliv i Rakkestad kommune de nærmeste 4 år

A. Nærmiljøanlegg

K:	Kommunalt tilskudd	MM:	Miljømidler
*):	Bevilgede midler	S:	Spillemidler
P:	Private midler	x:	Søknadssum

		Anleggstart -finansiering											
Anlegg Tilrettelegging	**Kostn. i 1.000 kr**	**2012**			**2013**			**2014**			**2014**		
		K	**S**	**P**	**K**	**S**	**P**	**K**	**S**	**P**	**K**	**S**	**P**
Aktivitetsbane ved Rakkestad ungdomsskole	700'				500'	200'							

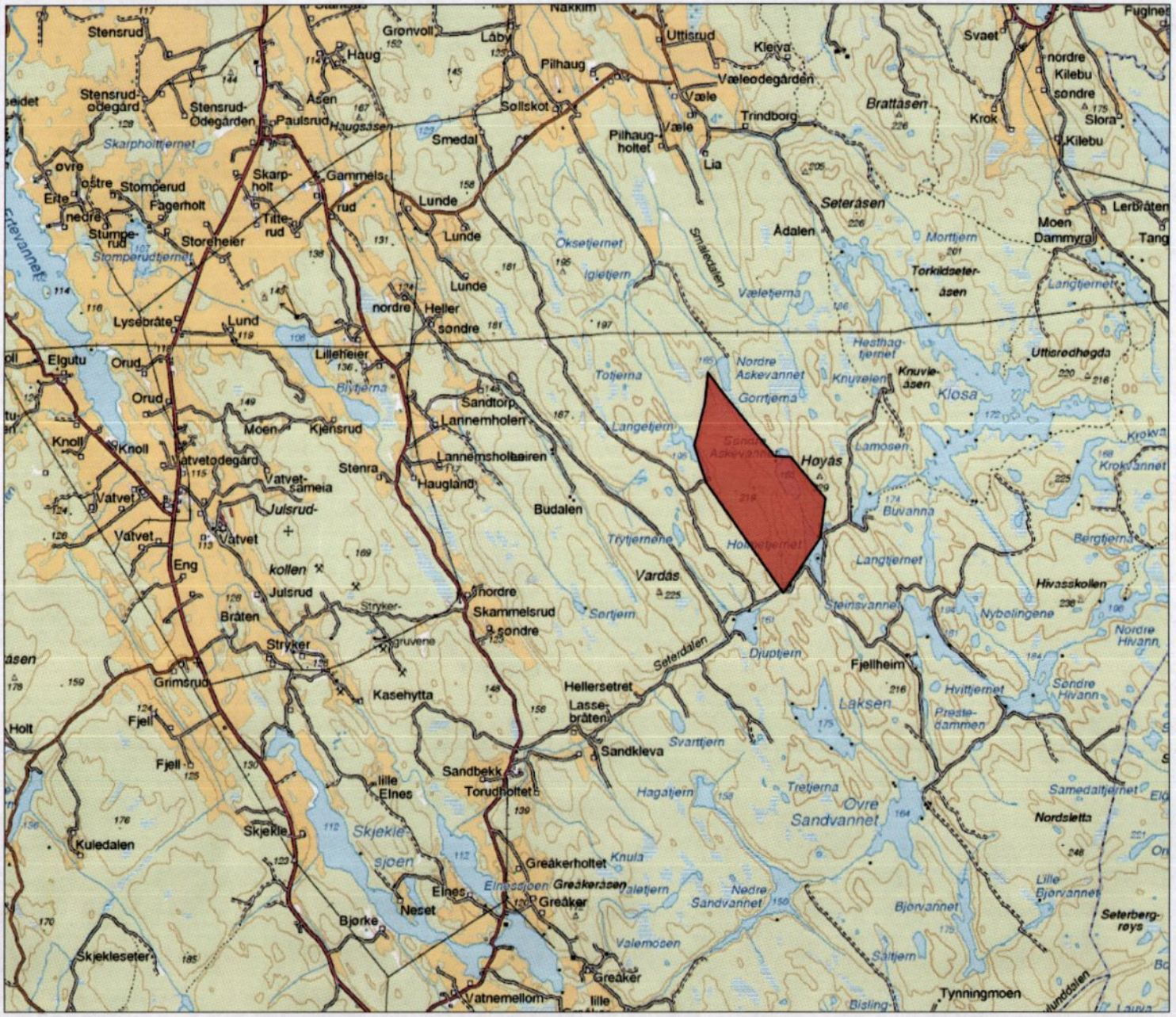
Vedlegg 1 KST sak 91/11

B. Ordinære anlegg (OA) og rehabiliteringsanlegg MED MER

K:	Kommunalt tilskudd	P:	Private midler
MM:	Miljømidler	S:	Spillemidler
*):	Bevilgede midler	x:	Søknadssum

		Anleggstart –finansiering											
Anlegg Tilrettelegging	**Kostn. i 1.000 kr**	**2012**			**2013**			**2014**			**2015**		
		K	**S**	**P**	**K**	**S**	**P**	**K**	**S**	**P**	**K**	**S**	**P**
Rehabilitering av Degerneshallen	500’		150’	350’									
Okart: Haraldstad syd	165’		55’	110’									
Blytjern skytebane Elektroniske skiver 100m	540’		180’	360’									
Blytjern skytebane felthurtigbane	480’		160’	320’									

DinSkog.no Utskrift



Tegnforklaring

- Annet Tillegg
- DEKNINGSPOLYGON
- Vern
- N50
  - Red: Band_1
  - Green: Band_2
  - Blue: Band_3
- N250
  - Red: Band_1
  - Green: Band_2
  - Blue: Band_3

1: 50 571

Kommentar

Vedlegg 1.

VEDLEGG 2 Tabell over aktuelle utbyggingsoppgaver i Rakkestad kommune i 10 – 12 års perspektiv
Uprioritert liste over langsiktige behov for anlegg og områder for idrett og friluftsliv i Rakkestad kommune 2012 – 2023.
Kategori: N = nærmiljøanlegg. OA = ordinære anlegg . R = rehabiliteringsanlegg

KAT	ANLEGGSTYPE	STED	EIER/UTBYGGER	ANSLÅTT UTBYGGINGS-KOSTNAD	ANSLÅTTE DRIFTSUTG. PR ÅR	KOMMENTAR
OA	O-kart	Revidering av Galborgen	Skaukam	Kr 150 000		
OA	O-kart	Nytegning rundt Bjørnstad camping	Skaukam	Kr 170 000		
OA	O-kart	Revidering av Rakkestad sentrum	Skaukam	Kr 50 000		
OA	O-kart	Revidering av Jonsrud	Skaukam	Kr 50 000		
OA	O-kart	Revidering av Kirkeng skole	Skaukam	Kr 50 000		
OA	O-kart	Revidering av Bredholtkartet	Skaukam	Kr 50 000		
OA	O-kart	Nytegning av Stikksmoen	Skaukam	170 000		
OA	Belysning	Os Idrettspark	Oshaug	Kr 800 000		
OA	Flytte duepress på lerduebane	Slettemoen	RDJFF	Kr 300 000		
OA	7-er bane kunstgress	RIF-anlegget	RIF	?		
OA	Rideanlegg – vannforsyning	Haugstad	Rakkestad kjøre og rideklubb	Kr 200.000		
N	Dørjestien - forlengelse	Dørja	Rakkestad kommune	?		
N	Friplassen, friidrettsanlegg	RIF-anlegget	RIF	?		

Vedlegg 2 KST sak 91/11

Vedlegg 2.

VIKEN SKOG

Rakkestad kommune v/Knut Østby
Postboks 264
1890 Rakkestad

Kongsberg 7. juli 2011

Vår saksbehandler:
Svein Ekanger, tlf. 90 62 12 40

Vår ref.:
Prosj. 1512

Deres ref.:

Frivillig vern ved Askevann – Anbefalt erstatningsforslag

På bakgrunn av min forrige erstatningsberegning og seinere tilbakemeldinger fra dere fremmet jeg et endelig krav og møtte statens skogsakkyndig til sluttforhandlinger i dag. Møtet endte opp med et anbefalt forslag til erstatning som oversendes alle parter for endelig godkjenning. Statens skogsakkyndig tar forbehold om aksept av resultatet fra Direktoratet for naturforvaltning.

Erstatningsberegningene er slik:

Eier	Staten/Heintz 23/6-11, kr	Ekanger 24/6-11, kr	Ekanger 6/7-11, kr	Forhandlingsres. 7/7-11, kr.
Rakkestad komm	1.495.572	1.588.159	1.661.103	**1.631.000**
Aanonsen	438.256	483.082	524.763	**522.000**
Sum	1.933.828	2.071.241	2.185.866	**2.153.000**

Jeg høynet mitt krav i forhandlingene fra mitt første oppsett på bakgrunn av informasjon fra begge eiere, primært om forhold knyttet til vedomsetning

Anbefalt erstatningsresultat ligger drøyt 11 % over statens første tilbud, drøyt 4 % over min første beregning og godt over hva jeg trodde ville være oppnåelig ved første utsending til dere. Jeg anser dette som et endelig resultat og tror ikke det er mulig å oppnå noe mer, slik sett anbefaler jeg sterkt at dere aksepterer dette.

Ved kontakt med dere nå de siste dagene ble vi enige om at det kan være aktuelt at vi møtes over sommerferien for å foreta en endelig gjennomgang og evt. avklaring av uklarheter før dere formelt tar stilling til om resultatet aksepteres. Jeg ber Knut Østby om å avklare om dere ønsker møte før dere tar endelig stilling, og i så fall koordinerer et møte f.eks. i uke 32 (etter 8. august).

Vedlagt følger detaljert beregning for deres areal i området for frivillig vern. De viktigste sakene vi fikk gjennomslag for i sluttforhandlingene, er knyttet til tømmerpriser og bonuser.

Følgende tømmerpriser er lagt inn:

- Gran : Sagtømmer kr. 480 / massevirke kr. 286
- Furu: Spesial fra frøtrær kr. 800 / spesial ellers kr 700 / sagtømmer kr. 450 / ved kr. 320 / massevirke kr. 250

E-post: se@viken.skog.no

Viken Skog BA	Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Bankkonto:
NO 988 983 772	Postboks 554 3605 Kongsberg	Baneveien 32B	+47 32 10 30 00		

Følgende sortimentsfordeling er avtalt:

- Gran: 70 % sagtømmer, 30 % massevirke
- Furu første hogst: 10 % spesial, 60 % sagtømmer, 15 % massevirke, 15 % ved
- Furu frøtrær: 20 % spesial, 60 % sagtømmer, 0 % massevirke, 20 % ved

Vi har mao fått inn at en god del av furu massevirke omsettes som ved, og til en pris som tilsvarer informasjon fra Knut Østby.

Etter aksept av forhandlingsresultat skal det inngås avtale om frivillig vern. For å spare tid i den videre prosessen har jeg derfor bedt Geir Hardeng hos Fylkesmannen i Østfold om å utarbeide vernekart og forslag til verneforskrift. Dette vil dere få til gjennomsyn så snart det foreligger. Når det er enighet om alt, kan det utarbeides og inngås avtale.

Jeg benytter anledningen til å ønske en god sommer!

Med vennlig hilsen
VIKEN SKOG BA

Svein Ekanger

Vedlegg: Erstatningsberegning for din eiendom

Vedlegg 3 KST sak 91/11

RAKKESTAD IDRETTSRÅDs UTTALELSE TIL PRIORITERT HANDLINGSPROGRAM 2012-2015

Sak 11/11 Styremøte fredag 14.11.2011

Behandling av kommuneplan og søknad om anleggsmidler.

Det er av kommunen innstilt på 4 prioriterte tiltak:

Rehabilitering av Degerneshallen	Degernes	Rakkestadhallene AS
O-kart:	Haraldstad syd	Skaukameratene O.lag
Elektroniske skiver 100m	Blytjern skytebane	Degernes skytterlag
Felthurtigbane	Blytjern skytebane	Degernes skytterlag

RIR gir tilslutning til kommunens prioritering.

RIR påpeker at det er ønskelig at skytterlagene ser på muligheten for samarbeid om baner og anlegg.

Liste over aktuelle utbyggingssaker for 10-12 års perspektiv betrakter RIR som ikke oppsatt i prioritert rekkefølge.
Det savnes flere tiltak fra lagene samt tiltak for uorganisert ungdom, som for eksempel en sentrumsnær flerbrukshall som også kan brukes til skate, freestyle sykkel og andre aktiviteter.
RIR betrakter ikke friplassen som nærmiljøanlegg pga begrenset offentlig tilgang.

Når det gjelder langtidsplan for anlegg er det ønskelig at det sees på muligheten for å få til regionalt anlegg i kommunen. Dette kan for eksempel være innen skyting, orientering og annet.

E.post 14.11.2011 / Arkivsak: 11/2292
RIR v/Eli Uttakleiv

Fylkesmannen i Østfold 7.11.2011. Utkast til vernebestemmelser

Verneplan for skog. Vern av Askevann naturreservat i Rakkestad kommune i Østfold fylke

Fastsatt ved kongelig resolusjon .....med hjemmel i lov 19. juni 2009 nr. 100 om forvaltning av naturens mangfold (naturmangfoldloven) § 34 jf. § 37 og § 62.
Fremmet av Miljøverndepartementet.

§ 1 Formål
Formålet med naturreservatet er å bevare et relativ lite påvirket skogområde, med tjern, myrer, gran- og furuskog. Området representerer en bestemt naturtype i lavereliggende trakter omkring marin grense på grunnfjellet i Sørøst-Norge. Området har betydning for biologisk mangfold.

§ 2 Geografisk avgrensing
Naturreservatet berører følgende gnr./bnr.: 136/2 og 137/4,5 i Rakkestad kommune.
Naturreservatet dekker et totalareal på ..... dekar.
Grensene for naturreservatet går fram av kart i målestokk 1:10.000 datert Miljøverndepartementet .....
De nøyaktige grensene for naturreservatet skal avmerkes i marka.
Knekkpunktene skal koordinatfestes.
Verneforskriften med kart oppbevares i Rakkestad kommune, hos Fylkesmannen i Østfold fylke, i Direktoratet for naturforvaltning og i Miljøverndepartementet.
Det samme gjelder jordskiftekartet som lages etter grensemerking.

§ 3 Vernebestemmelser
I naturreservatet må ingen foreta noe som forringer verneverdiene angitt i verneformålet. I naturreservatet gjelder følgende vernebestemmelser:

1. Vegetasjon, herunder døde busker og trær, er fredet mot skade og ødeleggelse. Det er forbudt å fjerne planter og sopp (inkludert lav) eller deler av disse fra naturreservatet. Planting eller såing av trær og annen vegetasjon er forbudt.
2. Dyrelivet, herunder reirplasser og hiområder, er fredet mot skade, ødeleggelse og unødig forstyrrelse. Utsetting av dyr er forbudt.
3. Området er vernet mot ethvert tiltak som kan endre naturmiljøet, som f.eks. oppføring av bygninger, anlegg, gjerder, andre varige eller midlertidige innretninger, parkering av campingvogner, brakker e.l., opplag av båter, framføring av luftledninger, jordkabler, kloakkledninger, bygging av veier, drenering eller annen form for tørrlegging, uttak, oppfylling eller lagring av masse, utføring av kloakk eller andre konsentrerte forurensningstilførsler, henleggelse av avfall, gjødsling, kalking eller bruk av kjemiske bekjempingsmidler. Forsøpling er forbudt. Opplistingen av tiltak er ikke uttømmende.
4. Bruk av naturreservatet til teltleirer, idrettsarrangementer eller andre større arrangementer er forbudt.
5. Etablering av båtplasser og bålbrenning er forbudt.
6. Oppsetting av kamuflasjeinnretninger er forbudt.

§ 4 Generelle unntak fra vernebestemmelsene
Vernebestemmelsene er ikke til hinder for:

1. Sanking av bær og matsopp.
2. Jakt, fangst og fiske i samsvar med gjeldende lovverk.
3. Skadefelling av store rovdyr i samsvar med gjeldende lovverk.
4. Beiting.
5. Bålbrenning med tørrkvist fra bakken eller med medbrakt ved, i tidsrommet 16. september - 14. april.
6. Vedlikehold og merking av stier avmerket på vernekartet.
7. Rydding av mindre mengder kvist på poster i samband med jakt på storvilt.
8. Utsetting av saltsteiner.

9. Vedlikehold av bekk i reservatgrensen sørvest for Holmetjern, etter at forvaltningsmyndigheten er varslet.

§ 5 Regulering av ferdsel

I naturreservatet gjelder følgende bestemmelser om ferdsel:

1. All ferdsel skal skje varsomt og ta hensyn til vegetasjon, dyreliv og kulturminner.
2. Motorisert ferdsel til lands og til vanns er forbudt, herunder start og landing med luftfartøy.
3. Utenom på eksisterende stier er bruk av sykkel, hest og kjerre samt ridning forbudt.

§ 6 Generelle unntak fra ferdselsbestemmelsene

Ferdselsbestemmelsene er ikke til hinder for:

1. Gjennomføring av militær operativ virksomhet og tiltak i forbindelse med ambulanse-, politi-, brannvern-, rednings- og oppsynsvirksomhet, samt gjennomføring av skjøtsels- og forvaltningsoppgaver som er bestemt av forvaltningsmyndigheten. Unntaket gjelder ikke øvingskjøring.
2. Nødvendig motorferdsel i forbindelse med uttransport av syke og skadde bufe. Kjøretøy som benyttes skal være skånsomt mot markoverflaten. Det skal gis melding til ansvarlig oppsyn for verneområdet i forkant av kjøring.
3. Nødvendig uttransport av felt elg og hjort med lett terrenggående beltekjøretøy som ikke setter varige spor i terrenget.

§ 7 Spesifiserte dispensasjonsbestemmelser

Forvaltningsmyndigheten kan etter søknad gi dispensasjon til:

1. Avgrenset bruk av naturreservatet for aktiviteter nevnt i § 3 nr. 4.
2. Istandsetting og vedlikehold av kulturminner.
3. Tiltak i forbindelse med forvaltning av vilt og fisk.
4. Nødvendig uttransport av felt elg og hjort med annet kjøretøy enn lett terrenggående beltekjøretøy som nevnt i § 6 nr. 3.
5. Oppsetting av gjerder i forbindelse med beiting.
   Nødvendig motorferdsel i forbindelse med aktiviteter nevnt i § 7 nr. 5.
9. Transport av ved, materialer og utstyr på frossen, snødekt mark eller med lett terrenggående beltekjøretøy som ikke setter varige spor i terrenget, langs vintervei / sti mellom Nordre og Søndre Askevann, til hytte på gnr./bnr. 136/15 nord i Søndre Askevann.

§ 8 Generelle dispensasjonsbestemmelser

Forvaltningsmyndigheten kan gjøre unntak fra forskriften dersom det ikke strider mot vernevedtakets formål og ikke kan påvirke verneverdiene nevneverdig, eller dersom sikkerhetshensyn eller hensynet til vesentlige samfunnsinteresser gjør det nødvendig, jf naturmangfoldloven § 48.

§ 9 Skjøtsel

Forvaltningsmyndigheten, eller den forvaltningsmyndigheten bestemmer, kan iverksette tiltak for å opprettholde eller oppnå den natur- eller kulturtilstand som er formålet med vernet, jf naturmangfoldloven § 47.

§ 10 Forvaltningsplan

Det kan utarbeides forvaltningsplan med nærmere retningslinjer for forvaltning av naturreservatet. Forvaltningsplanen kan inneholde nærmere retningslinjer for gjennomføring av skjøtsel.

§ 11 Forvaltningsmyndighet

Direktoratet for naturforvaltning fastsetter hvem som skal ha forvaltningsmyndighet etter denne forskriften.

§ 12 Ikrafttredelse

Denne forskriften trer i kraft straks.

Askevann NR i Rakkestad kommune

Erstatningsberegning

Eiendom: 137/4,5 Rakkestad kommune

Arealfordeling	Dekar
Produktivt	664
Skrap	13
Imp.	0
Tekn. imp.	2
Myr	57
AMS	0
Vann	39
Totalareal	775

Volum	Hogstklasse 4		Hogstklasse 5		Hogstklasse 4-5	
Tilvekst	Volum	Tilvekst	Volum	Tilvekst	Volum	Tilvekst
Gran	255	6	1112	22	1367	28
Furu	100	3	4548	59	4648	62
Lauv	0	0	0	0	0	0
Sum prod.	355	9	5660	81	6015	90
Furu, skrap			31		31	
Totalt	355	9	5691	81	6046	90

Avvirkning	Generelt		Furu, foryngelse		
Periode	År	Andel	Tiltak	År	Andel
1	5	100 %	Frøtrestilling	Generell plar	85 %
2	15	0 %	Hogst frøtrær	10 år etter	15 %

Utgangsvolum	Periode 1		Periode 2		Sum	
	Volum	Andel	Volum	Andel	Volum	Andel
Gran	1367	26 %	0	0 %	1367	23 %
Furu, første hogst	3951	74 %	0	0 %	3951	65 %
Furu, skrap	27	0 %	0	0 %	27	0 %
Furu, frøtrær	0	0 %	702	100 %	702	12 %
Lauv	0	0 %	0	0 %	0	0 %
Sum	5344	100 %	702	100 %	6046	100 %

Avvirkningsplan		Utg.-volum	Tilvekst	Bruttovol.	T/a/m, %	Fradrag, vol	Nettovol	Bonus aut. beregn.
Periode 1	År 5	5344	484	5829	13 %	758	5071	30
Periode 2	År 15	702	149	851	13 %	111	740	0

Lagt på ett års tilvekst for å få med tilvekst i 2011

Midlere tømmerpris	Periode 1			Periode 2		
Treslag	**Pris**	**Andel**	**Veid pris**	**Pris**	**Andel**	**Veid pris**
Gran	422	26 %	108	422	0 %	0
Furu, første hogst	426	74 %	317	426	0 %	0
Furu, frøtrær	494	0 %	0	494	100 %	494
Lauv	0	0 %	0	0	0 %	0
Sum			425			494

Kostnader lang terrengkjøring			
Transportavst.	700		
Intervall	**Avstand**	**Kr/m3,100m**	**Kr/m3**
400-1000 m	300	1,5	4,5
>1000 m	0	1	0
Sum			4,5

Skogkulturkostnad								
Bonitet	**23**	**20**	**17**	**14**	**11**	**8**	**6**	**Sum**
Kr/m3	30	25	20	15	10	0	0	
Volumandel	0 %	0,0 %	5,6 %	24,4 %	60,3 %	9,2 %	0,5 %	100,0 %
Kostnad, kr/m3	0	0	1,12	3,66	6,03	0	0	10,81

Netto tømmerpris	Periode 1 Gran kr/m3	Periode 1 Furu kr/m3	Periode 1 Alt kr/m3	Periode 2 Frøtrær kr/m3	
Bruttopris	422	426	425	494	
Bonus/etterbetaling	10	10	10	10	
Bonus volum	30	30	30	0	
Korr. tømmerpris	0	0	0	30	Bonus for frøtrær, hogger 2.000-4.000 m3/år
Basis hogst/kjøring	-115	-115	-115	-135	
Vansk. hogst/kjøring	0	0	0	0	
Lang kjøring	-5	-5	-5	0	Ikke tillegg for lang kjøring ved hogst av frøtrær
Skogkultur	-11	-11	-11	0	Ikke skogkultur for hogst av frøtrær
Måling	-5	-5	-5	-5	
Vegvedl.h.	-5	-5	-5	-5	
Adm.	-5	-5	-5	-5	
Netto	316	320	319	384	

Vedlegg 4.

Verdiberegning, slutthogst

	År	Nettovol	Nettopris	Disk.faktor	Verdi
Periode 1	År 5	5071	319	0,7835	1268391
Periode 2	År 15	740	384	0,4810	136703
Sum					**1405094**

Verdiberegning GROT, hkl. 4-5, bon 14 og bedre, < 500 m kjøring)

	År	Nettovol	Grot lm3/fm3	GROT, lm3	Nettopris	Disk.faktor	Verdi
Periode 1	År 5	863	0,7	604	30	0,7835	14201
Periode 2	År 15	0	1,7	0	0	0,4810	0
Sum							**14201**

Grunnverdi h.kl. 4-5

Forutsetter at hogst fordeler seg jevnt på arealene

Bonitet	Areal	Andel hogst	Norm.verdi	Driftsnetto	Disk.faktor	Verdi
År 5						
Bon. G23	0	100 %	331	3,19	0,7835	0
Bon. G20	0	100 %	196	3,19	0,7835	0
Bon. G17	12	100 %	111	3,19	0,7835	3332
Bon. G14	54	100 %	56	3,19	0,7835	7564
Bon. F11	244	100 %	22	3,19	0,7835	13427
Bon. F8-F6	89	100 %	6	3,19	0,7835	1336
År 15						
Bon. G23	0	0 %	331	3,19	0,4810	0
Bon. G20	0	0 %	196	3,19	0,4810	0
Bon. G17	12	0 %	111	3,19	0,4810	0
Bon. G14	54	0 %	56	3,19	0,4810	0
Bon. F11	244	0 %	22	3,19	0,4810	0
Bon. F8-F6	89	0 %	6	3,19	0,4810	0
SUM						**25659**

Grunn- og venteverdi h.kl. 1-3

Bestand	Bon	Hkl.	Alder	Areal	Norm.verdi	Driftsnetto	Tetthet	Disk.faktor	Verdi
64	F8	11	0	8,4	6	3,19	1	1	161
82	F8	11	0	21,9	6	3,19	1	1	419
86	F14	31	35	7,5	316	3,19	1	1	7566
89	F11	21	15	10,4	46	3,19	1	1	1527
90	F14	31	45	12,9	514	3,19	1	1	21168
92	F11	32	45	5,3	200	3,19	0,91	1	3079
95	F11	21	15	32,3	46	3,19	1	1	4743
97	F11	32	45	4,1	200	3,19	0,91	1	2382
98	G14	31	55	15,1	678	3,19	1	1	32684
102	F14	31	45	6,7	514	3,19	1	1	10994
106	F11	21	15	7,2	46	3,19	1	1	1057
111	F11	31	45	63	200	3,19	1	1	40225
113	G14	21	25	3,8	181	3,19	1	1	2196
114	G11	21	35	5	99	3,19	1	1	1580
117	G14	31	60	6,8	762	3,19	1	1	16542
120	F11	21	11	13,9	37	3,19	1	1	1642
123	G14	21	25	11,8	181	3,19	1	1	6818
124	G14	21	25	4	181	3,19	1	1	2311
134	F14	31	45	15,5	214	3,19	1	1	10589
138	G17	11	0	4,7	111	3,19	1	1	1665
142	G17	31	55	3,5	1372	3,19	1	1	15330
SUM				**263,8**					**184681**

Sum verdiberegning

Post	Verdi
Avvirkning h.kl. 4-5	1405094
GROT	14201
Grunnverdi h.kl. 4-5	25659
Grunn- og venteverdi h.kl. 1-3	184681
Samlet verdi	**1629634**

Forhandlingsresultat	
Verdi	**1631000**

Resultat etter sluttforhandlinger med statens skogsakkyndig Dag A. Heintz
Kongsberg 7/7-11 SE